Extremal Metric and Topological Properties of Vertex Transitive and Cayley Graphs

Thesis

Extremal Metric and Topological Properties of Vertex Transitive and Cayley Graphs

James Fraser

Submitted for the degree of
Doctor of Philosophy in Mathematics
The Open University
Milton Keynes, UK

April 2020

Abstract

We shall consider problems in two broad areas of mathematics, namely the area of the degree diameter problem and the area of regular maps.

In the degree diameter problem we investigate finding graphs as large as possible with a given degree and diameter. Further, we may consider additional properties of such extremal graphs, for example restrictions on the kinds of symmetries that the graph in question exhibits.

We provide two pieces of research relating to the degree diameter problem. First, we provide a new derivation of the Hoffman-Singleton graph and show that this derivation may be used with minor modification to derive the Bosák graph. Ultimately we show that no further natural modification of the construction we use can derive any other Moore or mixed-Moore graphs. Second, we answer the previously open question of whether the Gómez graphs, which are known to be vertex-transitive, are in addition also Cayley. In doing this, we also generalise the construction of the Gómez graphs and show that the Gómez graphs are the largest graphs for given degree and diameter following the generalised construction.

We also provide two pieces of research relating to regular maps. We aim to address the related questions of for which triples of parameters k, l and m there exist finite regular maps of face length k, vertex order l and Petrie walk length m. We then address the related question of determining for which n there exist regular maps which are self dual and self Petrie dual which have face length, vertex order and Petrie dual walk length n. We address both questions by constructions of regular maps in fractional linear groups, necessarily leading us to study some interesting related number theoretic questions.

Preface

Acknowledgements

I would first like to thank my supervisor Professor Jozef Širáň for his advice and guidance throughout my PhD. I can now look back at where I was when I began the PhD and appreciate the amount of progress I have made since then, and I can only now begin to appreciate the level of sheer fluency that some people attain in mathematical thinking. I want to thank him in particular for his patience with me, the encouragement he has given me throughout, and the level of independence he has given me to choose the ideas I pursued. The relationship that a PhD student has with their supervisor is probably the most important factor in them both enjoying and having a successful PhD, and for that I know I have been extremely lucky.

Second, I would like to give a particular thank you to Dr Grahame Erskine, a previous PhD student of Jozef's and a current Visiting Research Fellow with the Open University. Whenever I have been in doubt about any aspect of the PhD programme he has always given me help and kept me from feeling lost, and on numerous occasions he has also shared with me the work he produced at equivalent points in his PhD, which I have been able to use as example model work to help guide me.

I would also like to thank the mathematics department at the Open University, its staff and students, for the discussions, suggestions and encouragement given over many lunch times: Jakub Sliačan, Olivia Jeans, Robert Lewis, James Tuite, Phil Rippon, Toby O'Neil, Hayley Ryder, Robert Brignall, Gwyneth Stallard, Tim Lowe, Ben Mestel, Matthew Jacques, James Waterman, Vasso Evdoridou, Argyris Christodoulou, and Yannis Dourekas.

I would like to thank the Open University for having given me the opportunity to do this PhD. The program has been an incredible experience of intellectual freedom in pursuing the ideas I find interesting. It is not lost on me that very few people throughout human history have been in such a privileged position of sheer freedom, and the experience will undoubtedly be amongst the best periods of my life.

Lastly, I would like to thank my partner Yasmin, who I met on the first day of the PhD program. When I arrived I had imagined spending three years uninterrupted concentrating in an office, but that is not entirely how things transpired - for which I am retrospectively very grateful! You have undoubtedly had the largest impact on my

life of all during these three years - without which this document would undoubtedly be much longer and more tedious than it already is!

The completion of the thesis marks a point of change in one's life. At this point, I reflect on who I was when I arrived, and who I am now. It is clear to me that I have grown and matured in many ways, and that this was only possible because I have been surrounded by people who I admire and can aspire to be more like. Thank you to everyone, both mentioned above and inevitably who I've forgotten to mention, who has been part of my life during this time.

Declaration

Except for where otherwise stated, the results presented in this thesis represent my own work. In the case of joint work, I have taken the approach that contributions which are wholly or mainly my own are included without further comment. The parts of joint work which are primarily the work of others are summarised here with acknowledgement to the main author(s), and detailed results are omitted except where they aid in the exposition. Any omitted results may be found in cited work.

Contents

Chapter 1

Introduction

1.1 Notation

Before we begin, we introduce the notation which we make use of throughout. We use the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ to denote the natural numbers (taking $\mathbb{N} = \{0, 1, 2, \dots\}$), integers, rationals, reals and complex numbers respectively. We use the notation $\mathbb{Z}/n\mathbb{Z}$ to denote the integers modulo n. We use $\mathbb{M}(R)^n$ to denote the ring of $n \times n$ matrices over the ring R. We use $\mathrm{GF}(p^k)$ to denote the finite field on p^k elements unique up to isomorphism.

We define a graph as a tuple $G = \langle V, E \rangle$, where V is the set of *vertices* and E is the set of *edges*, we shall only consider finite graphs in which $|V|$ and $|E|$ are finite. When we refer to a graph G we may also use $\mathrm{V}(G)$ to denote the vertex set of G and $\mathrm{E}(G)$ to denote the edge set of G. We consider graphs which are *undirected*, *directed* or *mixed*. We shall refer to each as graphs relying on context to make clear which type we are talking about and explicitly clarifying when necessary. In particular, we will also use the term *digraph* to refer to directed graphs when appropriate. In short we refer to directed graphs as *digraphs*. For an undirected graph, members of the edge set are sets of the form $\{u, v\}$ where $u, v \in V$ are vertices and $u \neq v$. If $\{u, v\} \in E$ we write $u \sim v$ and say that u and v are *adjacent*. For a directed graph, members of the edge set are tuples of the form $\langle u, v \rangle$ for some $u, v \in V$. If $\langle u, v \rangle \in E$ we write $u \to v$ and say that u is adjacent to v. In a mixed graph we allow edges of both types. We note that the graphs we consider are *simple* graphs, as between any pair of vertices we allow at most one edge, and we also disallow loops (an edge from a vertex to itself).

Within a graph $G = \langle V, E \rangle$ we call a series of vertices $v_0, v_1, \dots, v_n$ a *path* if there exist edges in E such that v_i is adjacent to v_{i+1} for all $0 \leq i < n$. The *length* of a path is the number of edges in the path, hence the length of the path on the vertices $v_0, v_1, \dots, v_n$ is n. For two vertices $u, v \in V$ we define the *distance* from u to v as $\mathrm{d}(u, v) = 0$ if $u = v$, $\mathrm{d}(u, v) = \infty$ if there does not exist a path from u to v, and $\mathrm{d}(u, v)$ is the length of the shortest path from u to v otherwise. If between any pair of vertices $u, v \in V$ we always have $\mathrm{d}(u, v) < \infty$ then we say G is *connected*.

For an undirected graph $G = \langle V, E \rangle$ and a vertex v, we define the *degree* of v to be

the number of edges $e \in E$ such that $v \in e$. For a directed graph $G = \langle V, E \rangle$ and a vertex v, we define the *out degree* of v as the number of edges of the form $v \to u$ in E, and the *in degree* of v as the number of edges of the form $u \to v$ in E. We call an undirected graph $G = \langle V, E \rangle$ *regular* if all vertices $v \in V$ have the same degree. We call a directed graph $G = \langle V, E \rangle$ *out regular* if all vertices $v \in V$ have the same out degree, *in regular* if all vertices $v \in V$ have the same in degree, and *totally regular* if G is both out regular and in regular. For a mixed graph $G = \langle V, E \rangle$ we define the *undirected degree*, *in degree* and *out degree* in the obvious way, and call a mixed graph $G = \langle V, E \rangle$ *totally regular* if each vertex $v \in V$ has the same undirected degree, in degree and out degree.

For a graph $G = \langle V, E \rangle$, and some subset $V' \subseteq V$ of V, we define the *subgraph of G induced by V'* as the graph $G' = \langle V', E' \rangle$ where $E' \subseteq E$ is the set of edges in E which only contain vertices in V'.

For graphs $G = \langle V, E \rangle$ and $G' = \langle V', E' \rangle$ we call a function $\phi : V \to V'$ a homomorphism from G to G' if for any $u, v \in V$ such that u is adjacent to v in G, we have that $\phi(u)$ is adjacent to $\phi(v)$ in G'. We call a function $\phi : V \to V'$ an isomorphism if ϕ is a bijection and for all $u, v \in V$ we have u is adjacent to v in G if, and only if, $\phi(u)$ is adjacent to $\phi(v)$ in G'. For a graph $G = \langle V, E \rangle$ we call an isomorphism from G to itself an automorphism, and define the *automorphism group* of G, denoted $\mathrm{Aut}(G)$, as the set of automorphisms of G. The fact that this set forms a group is easily seen.

For a group Γ and some set $S \subseteq \Gamma$ we define the *Cayley* digraph of Γ and S, denoted $\mathrm{Cay}(\Gamma, S)$ as the digraph $G = \langle \Gamma, E \rangle$ with vertex set Γ, the members of the group Γ, and edge set E such that $g \to h$ if, and only if, $g^{-1}h \in S$. It can easily be seen that for any $g \in \Gamma$, one may define a function $\phi : G \to G$ by $\phi(h) = gh$ which is an automorphism of G. Hence, there exists some group $H \leq \mathrm{Aut}(G)$ with $H \cong \Gamma$. We call G *regular* if we have $\mathrm{Aut}(G) \cong \Gamma$. A simple but important property of Cayley digraphs is the following.

Proposition 1.1. *A digraph G is Cayley if, and only if, there is a subgroup H of its automorphism group $\mathrm{Aut}(G)$ acting regularly on the vertices of G.*

Proof. The result is standard and we only provide a sketch. The fact a Cayley digraph has such a subgroup of its automorphism group follows from what we have already said. For the other implication, if G is a digraph and $\Gamma \leq \mathrm{Aut}(G)$ is a subgroup of the automorphism group of G acting regularly on $\mathrm{V}(G)$ then we may fix an arbitrary vertex $v \in \mathrm{V}(G)$ and label each vertex $u \in \mathrm{V}(G)$ with the automorphism

$g \in \Gamma$ which maps v to u. We then take the set S to be the set of members of Γ associated with the neighbours of v. Then we have $\mathrm{Cay}(\Gamma, S) \cong G$. □

We pay particular attention to the *degree* and *diameter* of graphs. We define the *diameter* of a graph $G = \langle V, E \rangle$ as the maximum distance $\mathrm{d}(u, v)$ between any two vertices $u, v \in V$. We denote the degree of G by $\mathrm{Deg}(G)$ and the diameter of G by $\mathrm{Diam}(G)$. Throughout we typically use the letter k to denote the diameter of a graph and the letter d to denote the degree.

We call a graph $G = \langle V, E \rangle$ *k-geodetic* if for all $u, v \in V$ there is at most one path connecting u and v of length less than or equal to k. We refer to this property as *k-geodesity*.

Later we give complete definitions of *Moore graphs* and *mixed Moore graphs*. Here we simply note that we use the notation (d, k)-Moore graph to denote a Moore graph of degree d and diameter k, and (r, z, k)-mixed Moore graph to denote a mixed Moore graph of undirected degree r, directed degree z and diameter k.

We now define the following special graphs and groups. For any $n \in \mathbb{N}$, $n \geq 2$ we define the *cycle graph* $C_n = \langle V, E \rangle$ such that $V = \{v_1, v_2, \ldots, v_n\}$, v_i is adjacent to v_{i+1} and v_n is adjacent to v_1. For any $n \in \mathbb{N}$, $n \geq 1$, we define the *complete graph* $K_n = \langle V, E \rangle$ such that $V = \{v_1, v_2, \ldots, v_n\}$ and v_i is adjacent to v_j for all i, j. We note that these definitions are equally applicable for directed and undirected graphs, and we refer to a directed version of a graph C_n as a *directed cycle*. We use the notation S_n, A_n, $\mathrm{PSL}(n, p^k)$ and $\mathrm{PGL}(n, p^k)$ to denote symmetric groups, alternating groups, and projective linear groups in the usual way.

We use $\varphi(n)$, $\mathrm{d}(n)$, $\mu(n)$ to denote Euler's totient function, the divisors function and the Möbius function respectively. We use $\mathrm{rad}(n)$ to denote the *radical* of n, i.e. the product of the distinct prime factors of n. We use $\mathrm{ord}(g)$ to denote the order of an element g of a group, ring, field etc. This will usually be the multiplicative order of the element, though will be clarified in context if necessary.

We use the notation $\Phi_n(x)$ to denote the n^{th} cyclotomic polynomial, whose roots are the n^{th} primitive roots of unity. We use ξ_n to denote an n^{th} primitive root of unity, and ξ to denote a primitive root of unity when the order is not important. We use $\Psi_n(x)$ to denote the polynomial satisfying the identity $\Phi_n(x) = x^{\varphi(n)/2}\Psi_n(x + x^{-1})$. This polynomial first appears in the literature in [37] of Lehmer. We denote roots of $\Psi_n(x)$ as $\omega_n = \xi_n + \xi_n^{-1}$.

For natural numbers n and k and a prime p, we say p^k *exactly divides* n, and write

$p^k \mid\mid n$, if $p^k \mid n$ and $p^{k+1} \nmid n$. For natural numbers n and m we use (n, m) to denote the greatest common factor of n and m, and $[n, m]$ to denote the least common multiple of n and m.

For a matrix $M \in \mathbb{M}^n$ we define $\mathrm{tr}(M)$, the *trace* of M, as the sum of the elements on the diagonal of M. We use $\mathrm{Det}(M)$ to denote the *determinant* of M.

For rings R and S we use $R \oplus S$ to denote the *direct product* of R and S.

For a polynomial $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n$ we use $\deg(f(x)) = n$ to denote the *degree* of $f(x)$. We call $f(x)$ *monic* if $c_0 = 1$, and say $f(x)$ is *irreducible* if there exist no polynomials $g(x)$ and $h(x)$ such that $f(x) = g(x)h(x)$ where both $\deg(g(x)) > 1$ and $\deg(h(x)) > 1$. We use $\rho(f)$ to denote the multiset of roots of $f(x)$ counted with multiplicity. We also define $\mathrm{M}(f)$, the *Mahler measure* of $f(x)$, as the product $\prod_{\alpha \in \rho(f)} \max(1, |\alpha|)$, i.e. the product of the absolute value of all roots of f greater than 1.

For two polynomials $f(x)$ and $g(x)$ we define the *resultant* of $f(x)$ and $g(x)$ as

$$\prod_{\substack{\alpha \in \rho(f) \\ \beta \in \rho(g)}} (\alpha - \beta),$$

and denote it as $\mathrm{Res}(f, g)$. For a polynomial $f(x)$, we define the *discriminant* of $f(x)$ as $\mathrm{Res}(f, f')$, and denote it Δ_f.

For a field K and irreducible polynomial $f(x) \in K[x]$ with $\deg(f(x)) > 1$, we may call α a root of $f(x)$ and denote by $K(\alpha)$ the unique to isomorphism algebraic extension of K by a root of $f(x)$ isomorphic to $K[x]/\langle f(x) \rangle$. We denote by $[K(\alpha) : K]$ the *degree* of the field extension, given by $[K(\alpha) : K] = \deg(f(x))$. For fields K and L such that $K \leq L$, we denote by $\Gamma(L/K)$ the *Galois group* of L over K, that is the group of automorphisms of L which fix K.

1.2 Results

Before we begin, we first provide a summary of the original results of this thesis. This section relies on some definitions which are made at the start of the corresponding chapters. We present results relating to three distinct problem areas: the construction of Moore graphs; the degree-diameter problem and Cayley graphs; and the existence of regular maps with prescribed vertex, face and Petrie orders.

1.2.1 The Construction of Moore Graphs

Relating to the construction of Moore graphs we provide an original construction of the Hoffman-Singleton graph, from which we may easily determine properties such as vertex transitivity of the Hoffman-Singleton graph and characterise its automorphism. This result is given as Proposition 3.16 and covers all work within that section.

This method of construction is then applied to the case of the Bosák graph in which case we derive analagous results. Our principle result regarding the Bosák graph is given in Proposition 3.27, and covers the work from the same section.

We then determine the limits of our method of construction, which we use to derive the Petersen, Hoffman-Singleton, Bosák and the unique $(1, 1, 2)$-mixed Moore graph, and show that our method cannot be used to cover any other cases. We present this result as Proposition 3.38.

We also note that throughout our exposition we show a fundamental similarity between the open problems of whether there exists a $(57, 2)$-Moore graph and whether there exists a $(21, 1, 2)$-mixed Moore graph.

The results concerning derivation of the Hoffman-Singleton and Bosák graphs and their automorphism groups are known results.

1.2.2 The Degree-Diameter Problem and Cayley Graphs

In this section we study the Gómez graphs, and in particular we provide a solution to the open problem of when the Gómez graphs are Cayley graphs. This problem is of interest in the degree-diameter problem because if the Gómez graphs were Cayley they would provide extremal examples of Cayley graphs for given degree and diameter.

Ultimately the question of determining when Gómez graphs are Cayley graphs requires determining the automorphism groups of the Gómez graphs. We provide the result in Proposition 4.63 and Proposition 4.77.

Further, the Gómez graphs have a naturally similar definition to the Faber-Moore-Chen graphs, and the Faber-Moore-Chen graphs have been classified as Cayley or not by determining their automorphism groups. Hence, we provide a definition for a family of graphs called the word graphs, and derive our results by providing generalised methods which may also be applied to the Faber-Moore-Chen graphs. We show that Gómez graphs and Faber-Moore-Chen graphs are examples of what we call shift restricted word graphs, and provide a further result to show that the Gómez graphs are the largest possible graphs for given degree and diameter

amongst the shift restricted word graphs. We provide this result in Proposition 4.15.

1.2.3 Existence of Regular Maps for Prescribed Vertex, Face and Petrie Orders

Finally we investigate the open problem of determining for which triples $(k, l, m) \in \mathbb{N}^3$ there exist (k, l, m)-regular maps. We provide a partial resolution to the conjecture that, for all but finitely many triples (k, l, m), there exists a (k, l, m)-regular map. Further, after deriving this result we apply our methods to the question of determining for which k there exist (k, k, k)-regular maps which are both self-dual and self-Petrie-dual.

In our derivation of our partial solution, we in particular prove the following result which has not been seen by the author in the literature (except on a web forum, cited in the thesis).

Proposition. For any monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $x \nmid f(x)$ and $\Phi_n(x) \nmid f(x)$ for all n there are only finitely many $m \in \mathbb{N}$ such that $f(x)$ has no root of order m in any finite field.

We also provide a constructive method of determining the set of all such m for which there exists no root of $f(x)$ of order m in any finite field. We present this result as Proposition 6.57, and work in the subsequent section shows how we may construct the set of values m. Also, in the opinion of the author, it is worth noting that the objects referred to as *Galois rings* used for generalising some results to also cover cases involving algebraic elements are an original invention of the author. These objects share some similarities with the p-adic numbers.

In addition to this, our work is related to work on determining behaviour of Fibonacci and Fibonacci-like sequences modulo a prime. In developing our tools, we also find we may apply them to determine precisely for which m there exists a prime p such that a k-Fibonacci sequence has period m modulo p. This is similar, but distinct to, the known results concerning apparitions in the area. The author is not familiar with equivalent results to the ones derived in this thesis within the literature. We provide these results in Proposition 6.52 and Proposition 6.53.

We provide our partial solution, namely that for any given pair (k, l) there are only finitely many m such that no (k, l, m)-regular map esists, in Proposition 6.77. Finally, we apply our methods to the case of self-dual and self-Petrie-dual (k, k, k)-regular maps in the final chapter, and derive our result in Proposition 7.10. This application of our earlier results does not in itself provide a new result, but does provide another

method of showing that, for all k except $k = 3$, there exists a self-dual and self-Petrie-dual (k, k, k)-regular map.

1.2.4 Publication of Results

At the current time of writing, none of the results or work in this thesis is published. The work from the chapter on word graphs is available in a very similar form on arXiv.

Chapter 2

Background to the Degree-Diameter Problem

We shall begin our work by investigating the degree-diameter problem. The degree-diameter problem forms a large area of research of which we shall only cover a small fraction. For an introduction to the area as a whole the reader may refer to the survey paper [43] of Miller and Širáň.

The degree-diameter problem originates from considering the question: for a given maximum vertex degree d and diameter k how large can a graph be? The question was originally posed by Moore based on the following observation.

Proposition 2.1. *A graph G of maximum vertex degree d and diameter k has at most $\mathrm{M}(d,k)$ vertices, where $\mathrm{M}(d,k)$ is given by*

$$\mathrm{M}(d,k) = \begin{cases} 1 + d\frac{(d-1)^k - 1}{d-2} & \text{if } d > 2, \\ 2k+1 & \text{if } d = 2. \end{cases} \tag{2.1}$$

Proof. This bound is trivially achieved by considering a breadth-first-search tree starting from an arbitrary vertex of G. In the first layer there is 1 vertex, at the second there are at most d vertices, in the third at most $d(d-1)$ vertices etc. At the k^{th} layer we must have found all of the vertices as the diameter of the graph is k. This gives a bound of the form $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$ which simplifies to our expression for $\mathrm{M}(d,k)$. □

This bound is called the *Moore bound*, and a graph which achieves the Moore bound is called a *Moore graph*. We see that in the case $d = 2$ the odd length cycle C_{2k+1} achieves the Moore bound, and in the case $k = 1$ the complete graph K_{d+1} achieves the Moore bound. We shall call the graphs C_{2k+1} and K_k *trivial* Moore graphs. In the paper [31] of Hoffman and Singleton it was shown via algebraic methods that for diameter $k = 2$ there are no non-trivial Moore graphs for any degree $d \neq 3, 7, 57$ and that there are no non-trivial Moore graphs for diameter $k = 3$. For diameter $k = 2$ and degree $d = 3$ they showed there is a unique Moore graph, the Petersen graph, and for diameter $k = 2$ and degree $d = 7$ there is a unique Moore graph, which is now

known as the Hoffman-Singleton graph. Subsequently Bannai and Ito in [6], and independently Damerell in [18], extended the argument of Hoffman and Singleton to show that there are no non-trivial Moore graphs for any diameter $k > 2$. The remaining open case of degree $d = 57$ and diameter $k = 2$ has become one of the most famous open problems in algebraic graph theory.

Since these early results the study of the degree-diameter problem has been expanded to consider cases of different classes of graphs (e.g. directed, vertex-transitive, Cayley etc), and determining families of graphs as large as possible for given degree and diameter.

In our work we consider the degree-diameter problem for digraphs. In the case of digraphs we shall consider how large a graph can be with a maximum out degree d and maximum diameter k. With this definition, we obtain the following directed Moore bound.

Proposition 2.2. *A digraph G of maximum vertex out degree d and diameter k has at most* $\mathrm{DM}(d,k)$ *vertices where* $\mathrm{DM}(d,k)$ *is given by*

$$\mathrm{DM}(d,k) = \begin{cases} \frac{d^{k+1}-1}{d-1}, & \text{if } d > 1, \\ k+1, & \text{if } d = 1. \end{cases} \tag{2.2}$$

Proof. As before we consider a breadth first search tree rooted at an arbitrary vertex of G. In the first layer there is 1 vertex, in the second there are at most d, in the third at most d^2 etc. This gives a Moore bound of the form $1 + d + d^2 + \cdots + d^k$, which simplifies to our expression for $\mathrm{DM}(d,k)$. □

It was first shown by Plesník and Znám in [46] in 1974, and later independently by Bridges and Toueg in [8] in 1980 that there are no non-trivial Moore digraphs. Therefore, we aim to study the directed case of the degree-diameter problem by finding digraphs which are asymptotically close to the directed Moore bound, i.e. a family of graphs $G(d,k)$ for arbitrary maximum out degree d and diameter k such that $|\,\mathrm{V}(G(d,k))| \sim d^k$ when either d or k is fixed and the other tends to infinity.

As a result, finding digraphs of maximum out degree d and diameter k close to the directed Moore bound $\mathrm{DM}(d,k)$ has formed a significant area of research, and the best known results are maintained online [40]. The largest known digraphs approaching the directed Moore bound are not vertex-transitive, so it is also interesting to consider the further restriction of the degree-diameter problem to vertex-transitive digraphs. With this further restriction, the digraphs described by

Gómez in [29] are the largest known vertex-transitive digraphs approaching the directed Moore bound, and shall be a major topic for our research.

First, as the Gómez graphs are vertex-transitive, it is possible that they are also Cayley graphs. If the Gómez graphs were Cayley then they would also be the best known Cayley digraphs approaching the directed Moore bound. Hence, we shall answer the question of whether the Gómez digraphs are Cayley digraphs.

Second, the definition of the Gómez digraphs comes from a refinement of the definition of the Faber-Moore-Chen digraphs introduced in [24, 25]. Therefore, another question we shall answer is whether further refinements are possible to this definition to create digraphs with better asymptotic behaviour. We shall address this question by generalising the definition of the Faber-Moore-Chen digraphs and the Gómez digraphs and show that the Gómez digraphs achieve a natural definition of optimality within this generalised context.

Chapter 3

Moore Graphs

3.1 Introduction

In this chapter we shall examine in detail the derivation of some known results concerning Moore graphs and mixed Moore graphs. In particular we shall aim to show a fundamental similarity between the existence of Moore graphs and the existence of mixed Moore graphs with directed out-degree 1. We note that mixed Moore graphs of directed out-degree 1 have already received independent attention in [39] of López and Pujolàs. First, we quote standard results of Moore and mixed Moore graphs. We have that, for diameter $k = 2$, non-trivial (d, k)-Moore graphs may only exist for degree $d = 3, 7$ or 57. In the cases of degree $d = 3$ and 7 it is known that unique, highly symmetric Moore graphs exist with these parameters. In the case of degree $d = 57$ it was shown that a $(57, 2)$-Moore graph cannot be vertex transitive by Higman in an unpublished lecture, and it has been further shown that the automorphism group of a $(57, 2)$-Moore graph can have at most 375 members by Mačaj and Širáň in [41]. We will draw a similarity between what happens in this case of Moore graphs and the case of (r, z, k)-mixed Moore graphs where we consider the directed degree $z = 1$ and the diameter $k = 2$. In this case it is known that mixed Moore graphs may only exist for undirected degree $r = 1, 3$ or 21 (this result may be extracted from [7]. In the cases of undirected degree $r = 1$ and $r = 3$ it is known that unique mixed Moore graphs exist with the given parameters and that they are vertex transitive. In the case of undirected degree $r = 21$ it is not known whether a $(21, 1, 2)$-mixed Moore graph exists, and equivalent results to those concerning the automorphism group of a potential $(57, 2)$-Moore graph are also not known.

It is of particular interest that the argument from which we derive the possible parameters for Moore graphs of diameter 2 used in [31] may be applied to the mixed Moore case of diameter 2 with no significant adjustments. Further, a $(21, 1, 2)$-mixed Moore graph would have only 486 vertices each with 22 neighbours, whereas a potential $(57, 2)$-Moore graph would have 3,250 vertices each with 57 neighbours. Hence, the problem of determining whether a $(21, 1, 2)$-mixed Moore graph exists occurs in a much smaller search space. Methods of optimised computer search have been used to show non-existence of some mixed Moore graphs in the paper [38] of

López, Miret and Fernández. Therefore, research into the case of a $(21, 1, 2)$-mixed Moore graph may be more accessible than research into a $(57, 2)$-Moore graph and help provide insight to the problem in general.

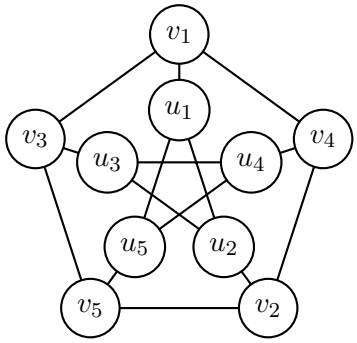
3.2 Existence Proofs for Small Parameters

We begin with proofs of uniqueness of the $(3, 2)$-Moore graph and the $(1, 1, 2)$-mixed Moore graph to show the similarity in these cases. In these cases the Moore bounds are 10 and 6 respectively. First we consider the $(3, 2)$-Moore graph.

Lemma 3.1. *Any diameter 2 Moore graph contains a 5-cycle.*

Proof. The definition we have taken for a (d, k)-Moore graph is that it is a graph of degree d and diameter k containing the number of vertices given by the Moore bound. From the derivation of the Moore bound, this means that a breadth first search tree from any vertex in such a graph encounters all other vertices at depth two with no repetition. Therefore such a graph is at least girth 5. Further, any edge not in the breadth first search tree must create either a 3, 4 or 5-cycle, so from girth considerations must create a 5-cycle, showing that a diameter 2 Moore graph contains at least one 5-cycle. □

Proposition 3.2. *There is a $(3, 2)$-Moore graph which is unique up to isomorphism.*



Proof. Suppose that G is a $(3, 2)$-Moore graph. Let $U = \{u_1, u_2, u_3, u_4, u_5\}$ be any 5-cycle in G such that $u_i \sim u_{i+1}$ (and $u_5 \sim u_1$ for the special case $i = 5$). As G is degree 3, each u_i must have another neighbour. As G is girth 5 this neighbour cannot be in U, and also each u_i must have a distinct neighbour. We shall label each neighbour of u_i as v_i. Now, considering that G is diameter 2, there must be a path of length at most 2 from u_1 to v_3. Due to the restriction on degree, we see that this is only possible if $v_1 \sim v_3$. By symmetry we deduce that $v_i \sim v_{i+2}$ (with $v_4 \sim v_1$ and $v_5 \sim v_2$ in the special cases). This uniquely determines the graph G. □

We see there is a unique $(3, 2)$-Moore graph. This graph is the Petersen graph. With a little extra effort we may show that this graph is vertex transitive, with automorphisms characterised by mapping any 5-cycle to any other 5-cycle of the graph in any rotation and orientation.

We now move onto the case of a $(1, 1, 2)$-mixed Moore graph.

Lemma 3.3. *If G is a $(r, 1, 2)$-mixed Moore graph, then the graph of only the directed edges of G is composed of disjoint 3-cycles.*

Proof. To show this claim we show that an arbitrary directed edge of G is in such a 3-cycle. Let $u \to v$ be a directed edge of G. As G is diameter 2 we must have $\mathrm{d}(v, u) \leq 2$. If $\mathrm{d}(v, u) = 1$ then there is a 2-cycle from $u \to v$ and back to u, contradicting that G is a mixed Moore graph. Therefore, we have $\mathrm{d}(v, u) = 2$, so there must be some vertex w, such that either $v \to w$ or $v \sim w$ and either $w \to u$ or $w \sim u$. This gives us four possibilities which we consider separately.

Case i) $v \sim w \sim u$. In this case we have $w \sim u \to v$ and $w \sim v$, so there are two paths of length at most 2 joining w and v, contradicting that G is a mixed Moore graph.

Case ii) $v \sim w \to u$. In this case we have $w \to u \to v$ and $w \sim v$, so there are two paths of length at most 2 joining w and v, contradicting that G is a mixed Moore graph.

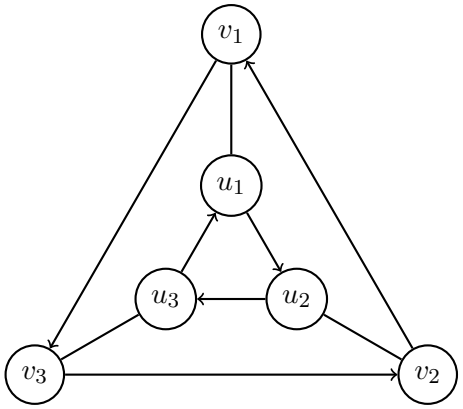
Case iii) $v \to w \sim u$. In this case we have $u \to v \to w$ and $u \sim w$, so there are two paths of length at most 2 joining u and w, contradicting that G is a mixed Moore graph.

Case iv) $v \to w \to u$. There is no contradiction in this case.

Hence, for each $u \to v$ we deduce the existence of some other vertex $w \in \mathrm{V}(G)$ such that $u \to v \to w \to u$, as required. □

We now prove the proposition corresponding to Proposition 3.2 for mixed Moore graphs.

Proposition 3.4. *There is a $(1, 1, 2)$-mixed Moore graph which is unique up to isomorphism.*



Proof. Assume that G is a $(1,1,2)$-mixed Moore graph. From Lemma 3.3 we may let $U = \{u_1, u_2, u_3\}$ be a directed 3-cycle in G such that $u_1 \to u_2 \to u_3 \to u_1$. As each vertex in G has both a directed and an undirected neighbour we must have that each u_i has another undirected neighbour. Further, by considering the girth of G we see that this neighbour cannot be in U, and that the undirected neighbours of each u_i must be distinct. Hence, let v_i be the undirected neighbours of each u_i. Now, as G is diameter 2 we must have that $d(u_1, v_3) \leq 2$. As we have already accounted for the neighbours of u_1 we have that $d(u_1, v_3) = 2$. Further, we see this is only possible if $v_1 \to v_3$. By symmetry we now deduce that $v_1 \to v_3 \to v_2 \to v_1$. This determines the graph G uniquely up to isomorphism. □

Altogether we see that the proof of the uniqueness of the $(3,2)$-Moore graph and that of the $(1,1,2)$-mixed Moore graph follow very closely, showing a similar structure of both graphs in which the 5 and 3-cycles labelled as U and V play corresponding roles. Later we shall see that this similarity is not isolated to this case.

3.3 The Hoffman-Singleton Graph

In this section we shall present a proof of the uniqueness up to isomorphism of the $(7,2)$-Moore graph, commonly known as the Hoffman-Singleton graph. In this case the Moore bound is 50. The proof we provide is an elementary combinatoric derivation. Another such derivation distinct to the one we present may be found in [32]. We shall also be able to count and characterise the automorphisms of the Hoffman-Singleton graph in a natural way following on from our derivation. In this section we assume that G is a $(7,2)$-Moore graph. Noting the result of Azarija and Klavžar that Moore graphs are extremal graphs containing a maximum number of convex cycles [2], we consider the Hoffman-Singleton graph in terms of the number of convex 5-cycles it contains.

Lemma 3.5. *The graph G contains 1,260 5-cycles.*

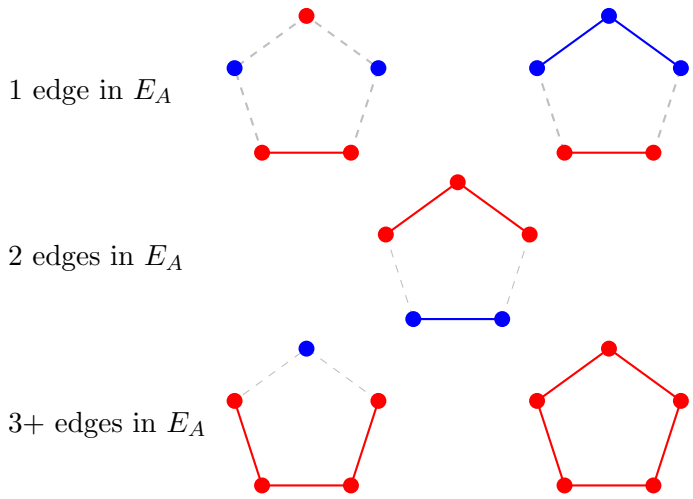
Proof. As G is 7 regular and the Moore bound tells us $|\,\mathrm{V}(G)| = 50$ we know that $|\,\mathrm{E}(G)| = 7 \times 50/2 = 175$. Consider a breadth first search tree T rooted at an arbitrary vertex $v \in \mathrm{V}(G)$. As there are 7 vertices in the 1^{st} layer of T and $6 \times 7 = 42$ vertices in the second layer of T there are 49 edges in T, so there are $175 - 49 = 126$ edges in $\mathrm{E}(G) \setminus \mathrm{E}(T)$. Now consider an edge $u \sim u'$ in $\mathrm{E}(G) \setminus \mathrm{E}(T)$. We must have $\mathrm{d}(v, u) = \mathrm{d}(v, u') = 2$ otherwise there would be a 3 or 4-cycle in G. Therefore there is a 5-cycle containing v and $u \sim u'$. We also have that any 5-cycle through v must contain an edge in $\mathrm{E}(G) \setminus \mathrm{E}(T)$. Hence there is a bijection between 5-cycles through v and edges in $\mathrm{E}(G) \setminus \mathrm{E}(T)$, giving that there are 126 5-cycles through v. As v was an arbitrary vertex, we may count all 5-cycles of G as $50 \times 126/5 = 1,260$. □

Lemma 3.6. *If $A, B \subseteq \mathrm{V}(G)$ with the following properties then the subgraphs of G induced by the vertices of A and B are composed of 5 disjoint 5-cycles.*

Property (i) $|A| = |B| = 25$;

Property (ii) $A \cap B = \emptyset$;

Property (iii) *A and B are 2-regular.*



Proof. Let G_A and G_B be the subgraphs of G induced by the vertices of A and B respectively. Let $E_A = \mathrm{E}(G_A)$, $E_B = \mathrm{E}(G_B)$ and $E_C = \mathrm{E}(G) \setminus (E_A \cup E_B)$. We now count the 5-cycles in G depending on how their edges are distributed between E_A, E_B and E_C. First, there are no 5-cycles whose edges are entirely in E_C, as any cycle of edges from E_C has its vertices alternating between A and B and therefore is even length.

Now we count 5-cycles with exactly one edge, say $u \sim v$, in E_A. Suppose that $u' \sim u$ and $v' \sim v$ with u' and v' in B. As G is diameter 2, we must have $\mathrm{d}(u', v') \leq 2$, and so $\mathrm{d}(u', v') = 2$ as otherwise we would have a 4-cycle. Therefore, for any edge $u \sim v$ in E_A there are 5 choices of u' and 5 choices of v' hence 25 5-cycles containing $u \sim v$. As $u \sim v$ was an arbitrary edge of E_A and there are 25 edges in E_A there are $25 \times 25 = 625$ 5-cycles with exactly one edge in E_A. By symmetry, there are 625 5-cycles with exactly one edge in E_B.

Now we consider 5-cycles with exactly 2 edges in E_A. First, by considering whether vertices of the cycle are in A or B, we notice that these edges must be consecutive, and that there must be 2 edges in E_C and the last edge in E_B. Therefore this 5-cycle has exactly one edge in E_B and we have already accounted for it in our counting.

Now we consider any 5-cycle with 3 or more edges in E_A. First, we notice that as G_A is 2-regular it must be made up of disjoint cycles. Consider any n-cycle in G_A. We have two cases.

Case (i) For any 5-cycle in G_A, there is 1 5-cycle with 3 or more edges in E_A namely this 5-cycle itself.

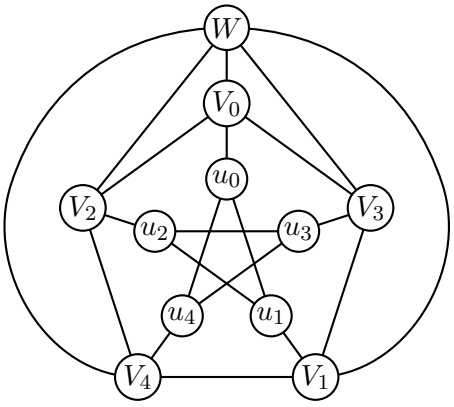
Case (ii) For any n-cycle in G_A where $n > 5$, consider any 3 consecutive edges in this n-cycle, say $u_0 \sim u_1 \sim u_2 \sim u_3$. We must have that $\mathrm{d}(u_0, u_3) = 2$, and so there is some $v \in \mathrm{V}(G)$ such that $u_0 \sim v \sim u_3$. Therefore $u_0 \sim u_1 \sim u_2 \sim u_3$ is in a 5-cycle. Further, we must have that $v \in B$ otherwise $u_0 \sim u_1 \sim u_2 \sim u_3$ would be in a 5-cycle in G_A. Hence for each 3 consecutive edges in the n-cycle there is a 5-cycle in G, which shows an n-cycle in G_A implies n 5-cycles in G.

If G_A is made of 5 disjoint 5-cycles then there are 5 5-cycles with 3 or more edges in E_A. Otherwise, there is at least one n-cycle in G_A where $n > 5$, and there are more than 5 5-cycles in G with 3 or more edges in E_A.

Finally, we have accounted for 1,250 5-cycles in G with less than 3 edges in E_A and less than 3 edges in E_B. From Lemma 3.5 there are 10 more 5-cycles with 3 or more edges in E_A or 3 or more edges in E_B. If either G_A or G_B is not made of 5 disjoint 5-cycles then there must be more than 10 such 5-cycles. Hence, we must have that G_A and G_B are both comprised of 5 disjoint 5-cycles. □

Lemma 3.7. *There exist sets of vertices $A, B \subseteq \mathrm{V}(G)$ such that $|A| = |B| = 25$, $A \cap B = \emptyset$ and the subgraphs of G induced by the sets A and B are both comprised of*

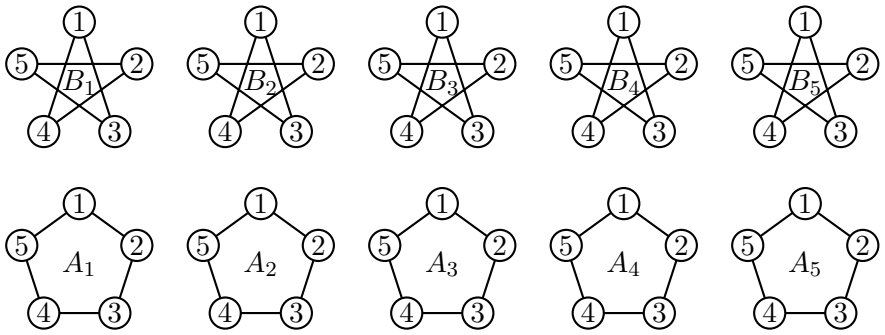
5 disjoint 5-cycles. Further, it is possible to choose an arbitrary 5-cycle U of G and then choose sets $A, B \subseteq \mathrm{V}(G)$ with the previous properties such that U appears in A.



Proof. Let $U = \{u_1, u_2, u_3, u_4, u_5\}$ be an arbitrary 5-cycle of G such that $u_i \sim u_{i+1}$ (with $u_5 \sim u_1$). As each vertex of G is degree 7 there are 5 unaccounted for neighbours of each u_i, say V_i. By the restrictions on the girth of G we have that $V_i \cap U = \emptyset$. We also have that $V_i \cap V_j = \emptyset$ for all $i \neq j$ by restrictions on girth. Therefore we have that $|V_i| = 5$. From the diameter of G, we know that $\mathrm{d}(u_1, v) \leq 2$ for all $v \in V_3$. As we have already accounted for all neighbours of u_1, u_2 and u_5 we see this can only be possible if there is some $w \in V_1$ with $w \sim v$. By making the same consideration for each $v \in V_3$, and noting that we cannot have some $w \in V_1$ and $v, v' \in V_3$ with $w \sim v$, $w \sim v'$ and $v \neq v'$ by girth, we see that for each $v \in V_3$ there is a unique $w \in V_1$ such that $v \sim w$. Letting $V = \bigcup V_i$ we see that there can be no further $v, v' \in V$ such that $v \sim v'$ other than those we have already derived, so the subgraph of G induced by vertices in V is regular of degree 2, and contains $|V| = \sum |V_i| = 25$ vertices. Now let $W = \mathrm{E}(G) \setminus (U \cup V)$. For any $w \in W$ we know that $\mathrm{d}(w, u_i) \leq 2$ by diameter, and so there must be some $v \in V_i$ such that $w \sim v$. By girth we know that there is at most one $v \in V_i$ such that $w \sim v$ for each i. Therefore w has 5 neighbours in V. As each vertex of G is degree 7, we know that each vertex $w \in W$ has two further neighbours in W. Altogether we see the subgraph of G induced by the vertices of W is regular of degree 2 and contains 20 vertices. Hence, letting $A = U \cup W$ and $B = V$ we have found two sets such that the subgraphs of G induced by A and B are regular of degree 2; A and B are disjoint; $|A| = |B| = 25$; and A contains an arbitrarily chosen 5-cycle of G. We now apply Lemma 3.6 and we are done. □

We have now derived the key fact that a $(7, 2)$-Moore graph must be divided into two even partitions of disjoint 5-cycles. This structure is particularly familiar from the simple pentagons and pentagrams construction of the Hoffman-Singleton graph due to Robertson. In light of this lemma, we now adopt the following notation for vertices in

our graph. We will let A and B be sets of 5 disjoint 5-cycles, with each 5-cycle being labelled A_i and B_i, and each vertex shall be labelled either $a_{i,j}$ or $b_{i,j}$ such that $a_{i,j} \in A_i$, $b_{i,j} \in B_i$, $a_{i,j} \sim a_{i,j\pm1}$ and $b_{i,j} \sim b_{i,j\pm2}$ as in the following diagram.



Lemma 3.8. *For all $1 \leq i, j \leq 5$, the subgraph of G induced by the vertices of A_i and B_j is isomorphic to the Petersen graph.*

Proof. Without loss of generality consider $i = j = 1$, and let $A_1 = \{a_1, a_2, a_3, a_4, a_5\}$ such that $a_i \sim a_{i+1}$ and $B_1 = \{b_1, b_2, b_3, b_4, b_5\}$ such that $b_i \sim b_{i+2}$. We first show that there must be some $a \in A_1$ and $b \in B_1$ such that $a \sim b$. From the fact $\mathrm{Diam}(G) = 2$, for any $a \in A_1$ and $b \in B_1$ we must have $\mathrm{d}(a, b) \leq 2$. If $\mathrm{d}(a, b) = 1$ then we are done, hence assume that $\mathrm{d}(a, b) = 2$. As $\mathrm{d}(a, b) = 2$ there must be some $v \in \mathrm{V}(G)$ such that $a \sim v \sim b$. First suppose that $v \in A$. If this is the case then from $a \sim v$ we have that $v \in A_1$ and v and b satisfy $v \in A_1$, $b \in B_1$ and $v \sim b$. Otherwise, we must have $v \in B$. In this case from the fact $v \sim b$ we have that $v \in B_1$, and a and v satisfy $a \in A_1$, $v \in B_1$ and $a \sim v$.

Now, without loss of generality we may label the vertices of A_1 and B_1 such that $a_1 \sim b_1$. We now consider how a_1 and b_2 are connected. If $a_1 \sim b_2$ then $a_1 \sim b_1 \sim b_4 \sim b_2 \sim a_1$ is a 4-cycle, contradicting the fact G is girth 5. Hence there is some vertex $v \in \mathrm{V}(G)$ such that $a_1 \sim v \sim b_2$. If $v \in B_1$, then we either have $v = b_4$ or $v = b_5$. If $v = b_4$ then $a_1 \sim b_4 \sim b_1 \sim a_1$ is a 3-cycle, contradicting that the girth of G is 5, and if $v = b_5$ then $a_1 \sim b_5 \sim b_3 \sim b_1 \sim a_1$ is a 4-cycle, contradicting that the girth of G is 5. Therefore we must have that $v \in A_1$. This gives the possibilities $v = a_2$ or $v = a_5$. In the case $v = a_5$ we apply the same argument to a_1 and b_5 and deduce that $a_2 \sim b_5$. In this case we may relabel B so that $a_2 \sim b_2$ and $a_5 \sim b_5$. Therefore, in all cases we may choose a labelling of B such that $a_1 \sim b_1$ and $a_2 \sim b_2$. Finally, once this is done we may deduce that $a_i \sim b_i$ for all $1 \leq i \leq 5$ by following the same logic. □

Corollary 3.9. *The graph G may have its vertices labelled such that $a_{1,j} \sim b_{i,j}$ and $a_{i,j} \sim b_{1,j}$ for all $1 \leq i, j \leq 5$.*

Proof. Immediate from the previous lemma. □

From here onwards we shall adopt the labelling of Corollary 3.9 for the labelling of the vertices of A and B.

Lemma 3.10. *If $a_{i,j} \sim b_{i',j'}$ then $a_{i,j+k} \sim b_{i',j'+k}$ for $1 \leq k \leq 4$ (with indices considered to wrap around).*

Proof. We first note that for $i = 1$ or $i' = 1$ we are done, so we assume that $i, i' \neq 1$. From Lemma 3.8 we know that the subgraph of G induced by the vertices of A_i and $B_{i'}$ is isomorphic to the Petersen graph. Hence, we must have that there is some j and j' such that $a_{i,j} \sim b_{i',j'}$, and either we have $a_{i,j+k} \sim b_{i',j'+k}$ or $a_{i,j+k} \sim b_{i',j'-k}$ for each $1 \leq k \leq 4$. Clearly, in the first case we are done, so assume $a_{i,j+k} \sim b_{i',j'-k}$. First, from our labelling we have that $a_{1,m} \sim b_{i',m}$ and $b_{1,m} \sim a_{i,m}$ for each $1 \leq m \leq 5$. Therefore if there is some n such that $a_{i,n} \sim b_{i',n}$ then there is a 4-cycle $a_{1,n} \sim b_{1,n} \sim a_{i,n} \sim b_{i',n} \sim a_{1,n}$, contradicting that G is girth 5. Now, as $a_{i,j} \sim b_{i',j'-k}$, we take the solution to $j + k \equiv j' - k \pmod 5$ for $0 \leq k \leq 4$, and take $n = j + k = j' - k$. Therefore, we cannot have $a_{i,j+k} \sim b_{i',j'-k}$ for $1 \leq k \leq 4$, from which the result follows. □

Corollary 3.11. *For every $1 \leq i, j \leq 5$ there exists some n such that $a_{i,k} \sim b_{j,k+n}$ for each $1 \leq k \leq 5$.*

Proof. The cases $i = 1$ or $j = 1$ are immediate, for $i, j \neq 1$ the result follows from the previous lemma. □

For each $1 \leq i, j \leq 5$ we shall refer to this n as the *offset* of A_i and B_j. We now define the matrix $M \in \mathbb{M}^5(\mathbb{Z}/5\,\mathbb{Z})$ such that $m_{i,j}$ is the offset of A_i and B_j. We shall call M the *offset matrix*. We note that the matrix M uniquely determines all edges of the graph G outside of G_A and G_B. Hence, for any $M \in \mathbb{M}^5(\mathbb{Z}/5\,\mathbb{Z})$ we define the graph G_M to be the graph with subgraphs G_A and G_B as in G, and the edges between vertices of A and B as implied by the matrix M.

We shall now define an equivalence relationship $\approx$ on matrices in $\mathbb{M}^5(\mathbb{Z}/5\,\mathbb{Z})$ which has the property that if $M \approx N$ then $G_M \cong G_N$. We define $\approx$ to be the transitive closure of the following.

i) $M \approx N$ for all $M, N \in \mathbb{M}^5(\mathbb{Z}/5\,\mathbb{Z})$ such that N can be formed by permuting the columns of M;

ii) $M \approx N$ for all $M, N \in \mathbb{M}^5(\mathbb{Z}/5\mathbb{Z})$ such that N can be formed by permuting the rows of M;

iii) $M \approx N$ for all $M, N \in \mathbb{M}^5(\mathbb{Z}/5\mathbb{Z})$ such that N can be formed by adding some $k \in \mathbb{Z}/5\mathbb{Z}$ to each entry in the first column of M;

iv) $M \approx N$ for all $M, N \in \mathbb{M}^5(\mathbb{Z}/5\mathbb{Z})$ such that N can be formed by adding some $k \in \mathbb{Z}/5\mathbb{Z}$ to each entry in the first row of M.

We now show that in each case if two matrices $M, N \in \mathbb{M}^5(\mathbb{Z}/5\mathbb{Z})$ are related by one of the above rules then $G_M \cong G_N$.

Lemma 3.12. *If $M \approx N$ then $G_M \cong G_N$.*

Proof. Suppose that M and N are related by precisely one of the rules (i), (ii), (iii) or (iv) defined above, we aim to show that $G_M \cong G_N$.

If $M \approx N$ are related by rule (i), suppose that $\pi \in S_5$ is the permutation such that column i of M is equal to column $\pi(i)$ of N. We now define the function $\phi : G_M \to G_N$ by $\phi(a_{i,j}) = a_{\pi(i),j}$ and $\phi(b_{i,j}) = b_{i,j}$ (abusing our notation of the sets A and B in graphs G_M and G_N). It can be shown that this function is an isomorphism from G_M to G_N and therefore $G_M \cong G_N$.

The case where $M \approx N$ are related by the rule (ii) is symmetric to the case where $M \approx N$ are related by rule (i).

If $M \approx N$ are related by rule (iii), suppose that $k \in \mathbb{Z}/5\mathbb{Z}$ such that $n_{i,0} = m_{i,0} + k$ for each $1 \leq i \leq 5$. In this case, let $\phi : G_M \to G_N$ be defined by $\phi(a_{i,j}) = a_{i,j}$ for $2 \leq i \leq 5$ and $1 \leq j \leq 5$, $\phi(b_{i,j}) = b_{i,j}$ and $\phi(a_{1,j}) = a_{1,j+k}$. It can be shown that this function is an isomorphism from G_M to G_N.

The case where $M \approx N$ are related by rule (iv) is symmetric to the case where $M \approx N$ are related by the rule (iii).

Finally, the result follows from the fact that the property of graph isomorphism is transitive. □

We now introduce a technical lemma to help us work with offset matrices and help us determine the requirements of an offset matrix for a $(7, 2)$-Moore graph.

Lemma 3.13. *If M is an offset matrix such that G_M is a Moore graph, then for any $x, y, i, j \in \mathbb{Z}/5\mathbb{Z}$ such that $x \neq y$ and $i \neq j$ we have $m_{x,i} - m_{y,i} \neq m_{x,j} - m_{y,j}$.*

Proof. First we create a matrix N such that $N \approx M$ by performing the following transformations on M.

i) permute the columns by some permutation $\pi \in S_5$ such that $\pi(i) = 1$ and $\pi(j) = 2$;

ii) permute the rows by some $\pi \in S_5$ such that $\pi(x) = 1$ and $\pi(y) = 2$;

iii) add $-m_{x,i}$ to column 1 and add $-m_{x,j}$ to column 2;

iv) add $-(m_{y,i} - m_{x,i})$ to row 2.

We illustrate the transformation with the following example.

$$M = \begin{pmatrix} - & - & - & - & - \\ - & m_{x,i} & - & m_{x,j} & - \\ - & - & - & - & - \\ - & m_{y,i} & - & m_{y,j} & - \\ - & - & - & - & - \end{pmatrix} \xrightarrow{i} \begin{pmatrix} - & - & - & - & - \\ m_{x,i} & m_{x,j} & - & - & - \\ - & - & - & - & - \\ m_{y,i} & m_{y,j} & - & - & - \\ - & - & - & - & - \end{pmatrix}$$

$$\xrightarrow{ii} \begin{pmatrix} m_{x,i} & m_{x,j} & - & - & - \\ m_{y,i} & m_{y,j} & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix} \xrightarrow{iii} \begin{pmatrix} 0 & 0 & - & - & - \\ m_{y,i} - m_{x,i} & m_{y,j} - m_{x,j} & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix}$$

$$\xrightarrow{iv} \begin{pmatrix} 0 & 0 & - & - & - \\ 0 & (m_{x,i} - m_{y,i}) - (m_{x,j} - m_{y,j}) & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix} = N.$$

Now, if $m_{x,i} - m_{y,i} = m_{x,j} - m_{y,j}$ then we have

$$N = \begin{pmatrix} 0 & 0 & - & - & - \\ 0 & 0 & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix}.$$

Hence, in G_N we have the 4-cycle $a_{1,1} \sim b_{2,1} \sim a_{2,1} \sim b_{1,1} \sim a_{1,1}$. Therefore, if G_N is a Moore graph, we cannot have $m_{x,i} - m_{y,i} = m_{x,j} - m_{y,j}$, as that would contradict

2-geodesity. Finally, as $G_M \cong G_N$ it follows that if G_M is a Moore graph we do not have $m_{x,i} - m_{y,i} = m_{x,j} - m_{y,j}$. □

We will now use our observations to create a standard form for the offset matrix, and prove that any $(7, 2)$-Moore graph with offset matrix is isomorphic to a $(7, 2)$-Moore graph with an offset matrix in standard form. We define our a standard form as follows. A matrix $M \in \mathbb{M}^5(\mathbb{Z}/5\,\mathbb{Z})$ is said to be in standard form if

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & - & - & - \\ 0 & 3 & - & - & - \\ 0 & 4 & - & - & - \end{pmatrix}.$$

Lemma 3.14. *If G_M is a $(7, 2)$-Moore graph with offset matrix M then there exists a matrix $N \in \mathbb{M}^5(\mathbb{Z}/5\,\mathbb{Z})$ such that $G_M \cong G_N$ and N is in standard form.*

Proof. We apply the following transformations on M to obtain a matrix N such that $G_M \cong G_N$ and N is in standard form. Between each step we rename the resulting matrix to M.

i) to each column i add $-m_{1,i}$ for $1 \leq i \leq 5$;

ii) to each row i add $-m_{i,1}$ for $2 \leq i \leq 5$;

iii) from Lemma 3.13 we have that each $m_{i,2}$ is distinct for $1 \leq i \leq 5$, so we may rearrange the columns of M by some permutation so that $m_{i,2}$ are in ascending order;

iv) finally we apply Lemma 3.13 to the rows instead of the columns as in the previous step.

The above steps transform M to standard form as illustrated as follows.

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix} \xrightarrow{i} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ b_1 & - & - & - & - \\ b_2 & - & - & - & - \\ b_3 & - & - & - & - \\ b_4 & - & - & - & - \end{pmatrix}$$

$$\xrightarrow{ii} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & c_1 & c_2 & c_3 & c_4 \\ 0 & - & - & - & - \\ 0 & - & - & - & - \\ 0 & - & - & - & - \end{pmatrix} \xrightarrow{iii} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & d_1 & - & - & - \\ 0 & d_2 & - & - & - \\ 0 & d_3 & - & - & - \end{pmatrix}$$

$$\xrightarrow{iv} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & - & - & - \\ 0 & 3 & - & - & - \\ 0 & 4 & - & - & - \end{pmatrix} = N.$$

□

Lemma 3.15. *There is only one matrix $M \in \mathbb{M}^5(\mathbb{Z}/5\mathbb{Z})$ in standard form such that G_M is a $(7,2)$-Moore graph.*

Proof. Suppose that $M \in \mathbb{M}^5(\mathbb{Z}/5\mathbb{Z})$ is in standard form and G_M is a $(7,2)$-Moore graph. We label the unknown entries of M as follows.

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & a & b & c \\ 0 & 3 & d & e & f \\ 0 & 4 & g & h & i \end{pmatrix}.$$

From Lemma 3.13 we can deduce that b cannot be any of 0, 2, 3 or 4, so we have $b = 1$. By symmetry, we also have $d = 1$. Continuing in this fashion we deduce that $a = 4$, $c = g = 3$, $f = h = 2$, $e = 4$ and $i = 1$. Altogether we have shown that M must be given by

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

□

We are now in a position to prove our first result concerning $(7,2)$-Moore graphs. (We note that we have not explicitly shown that the graph G_N is indeed a $(7,2)$-Moore graph, but as this is a trivial matter of verification we omit these details here).

Proposition 3.16. *There is a unique $(7,2)$-Moore graph up to isomorphism.*

Proof. From our work we have seen that if G is a $(7,2)$-Moore graph then there is an offset matrix M such that $G \cong G_M$; we have seen that if M is the offset matrix of a $(7,2)$-Moore graph then there is an offset matrix N of a $(7,2)$-Moore graph such that $G_M \cong G_N$ and N is in standard form; and finally we have seen that if N is the offset matrix of a $(7,2)$-Moore graph in standard form then N is uniquely defined. □

From this point forward we shall call the $(7,2)$-Moore graph the Hoffman-Singleton graph, and denote it by G for the rest of this section. We may now further expand on our work to characterise the automorphisms of G. We shall continue to use our notation of sets $A, B \subseteq \mathrm{V}(G)$, and shall take the edges of G to be those given by the unique offset matrix in standard form.

Lemma 3.17. *For each 5-cycle $U = \{u_1, u_2, u_3, u_4, u_5\} \subseteq \mathrm{V}(G)$ such that $u_i \sim u_{i+1}$, and each vertex $v \in \mathrm{V}(G)$ such that $\mathrm{d}(u_i, v) = 2$ for each u_i there is at most one automorphism $\phi \in \mathrm{Aut}(G)$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$.*

Proof. Suppose that $\phi : G \to G$ is an automorphism such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$. Considering the paths from $a_{2,1}$ to $a_{1,i}$ we have $a_{2,1} \sim b_{i,i} \sim a_{1,i}$, and considering the paths from v to u_i we have that there is a unique w_i for each u_i such that $v \sim w_i \sim u_i$ (both by 2-geodesity), so we must have $\phi(w_i) = b_{i,i}$ for each $1 \leq i \leq 5$. Let W be the set of vertices in $\mathrm{V}(G)$ which are distance 1 from any vertex in U (and not in U). By the reasoning of Lemma 3.7 we see that W is composed of 5 disjoint 5-cycles, each of which forms a Petersen graph with U. Call these 5-cycles such that $w_i \in W_i$, and relabel their vertices as $w_{i,j}$ such that $w_{i,i} = w_i$ and $w_{i,j} \sim w_{i,j\pm 2}$. Now, we have that each U and W_i induces a Petersen graph, and we know that $u_i \sim w_{i,i}$, so we deduce that $w_{i,j} \sim u_j$ for each $1 \leq i, j \leq 5$, and hence $\phi(b_{i,j}) = w_{i,j}$ is uniquely defined for each $b_{i,j}$.

From this we see that we may uniquely deduce the action of ϕ on all vertices in W from its action on U and v. By symmetry, we may deduce the action of ϕ on all members of $\mathrm{V}(G) \setminus W$ from its action on W. Therefore, we deduce the action of ϕ on all members of $\mathrm{V}(G)$. Hence, there is at most one automorphism $\phi \in \mathrm{Aut}(G)$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$. □

Lemma 3.18. *For each 5-cycle $U = \{u_1, u_2, u_3, u_4, u_5\} \subseteq \mathrm{V}(G)$ such that $u_i \sim u_{i+1}$, and each vertex $v \in \mathrm{V}(G)$ such that $\mathrm{d}(u_i, v) = 2$ for each u_i there is at least one automorphism $\phi \in \mathrm{Aut}(G)$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$.*

Proof. In the proof of Lemma 3.7 we may derive sets A and B such that $U \subseteq A$. Clearly, we may label the set A such that $a_{1,i} = u_i$. Now we can derive a labelling of

G with some offset matrix N such that $G \cong G_N$ with $u_i = a_{1,i}$ in the new labelling. We must have that $v \in A \setminus A_1$, so $v = a_{x,y}$ for some $2 \leq x \leq 5$ and $1 \leq y \leq 5$. Now we can apply a sequence of transformations to N to obtain a matrix M such that $G_N \cong G_M$ and the isomorphism from G_N to G_M fixes $a_{1,i}$ and maps $a_{x,y}$ to $a_{2,1}$.

In our transformation, we note that permuting the rows of N corresponds to permuting the 5-cycles A_i, so we may permute the rows of N to form N' move A_x to A_2 whilst fixing A_1. As a result we have $G \cong G_N \cong G'_N$ with an automorphism which relabels v as $a_{2,y}$. Now we note that adding k to row i of N' corresponds to mapping $a_{i,j}$ to $a_{i,j+k}$. Hence we transform N' to N'' by adding $1 - y$ to the second row of N'. This gives an isomorphism from G to $G_{N''}$ where $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$. Finally, the matrix N'' may be transformed to N''' in standard form by permuting the columns of N'' such that the first two rows of N''' are given as follows

$$N''' = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 \\ - & - & - & - & - \\ - & - & - & - & - \\ - & - & - & - & - \end{pmatrix}.$$

This can be followed by adding constants to and permuting the final three rows of N''' to get an offset matrix in standard form. Hence, we may deduce an isomorphism ϕ from G to G_M such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$. As M is in standard form Lemma 3.15 tells us that there is an automorphism from G_N to G in our original labelling, so there is a $\phi \in \mathrm{Aut}(G)$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$. □

Altogether, we may now count and characterise the automorphisms of the Hoffman-Singleton graph. The following results are known, we simply derive them as natural corollaries of our method of proof.

Proposition 3.19. *We have the following facts about the automorphisms of the Hoffman-Singleton graph.*

i) The automorphisms of the Hoffman-Singleton graph are uniquely characterised by their action on a 5-cycle and a single vertex at distance 2 from all points in the cycle.

ii) There are 252,000 automorphisms of the Hoffman-Singleton graph.

iii) The Hoffman-Singleton graph is vertex transitive.

Proof. The characterisation of the automorphisms of the Hoffman-Singleton graph follows immediately from the combination of Lemma 3.17 and Lemma 3.18. The vertex transitivity of the Hoffman-Singleton graph follows directly from Lemma 3.18. Finally, we may now count the automorphisms by counting 5-cycles, which we already did in Lemma 3.5; noting that for each 5-cycle there are 20 vertices at distance 2 from all vertices in the cycle; and noting that there are 10 possible labellings of any 5-cycle. This gives $10 \times 20 \times 1,260 = 252,000$ automorphisms of the Hoffman-Singleton graph. □

This concludes our characterisation of the automorphisms of the Hoffman-Singleton graph. An alternate geometric characterisation of the automorphisms of the Hoffman-Singleton graph can be found in the paper [30] of Hafner.

3.4 The Bosák Graph

In this section we aim to derive the uniqueness of the Bosák graph and the properties of its automorphism group analogously to our derivation of the Hoffman-Singleton graph and properties of its automorphism group. The Bosák graph is the unique $(3,1,2)$-mixed Moore graph. In this case the Moore bound tells us the Bosák graph has 18 vertices. It was shown to exist by Bosák in [7] and the uniqueness of the Bosák graph was shown by Nguyen, Miller and Gambert in [44].

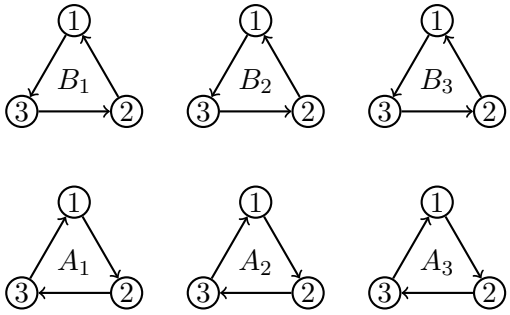
The first lemmas we have to establish the properties of the Hoffman-Singleton graph are to show that the Hoffman-Singleton graph must be decomposable into two partitions of 5 disjoint 5-cycles. In the Bosák graph, the directed 3-cycles of Lemma 3.3 will play a role analogous to the pentagons and pentagrams of the Hoffman-Singleton graph. Hence, we first aim to show that we may partition the directed 3-cycles of the Bosák graph into two sets such that the directed 3-cycles in each set are disjoint. We make this more formal as follows.

Lemma 3.20. *If G is a $(3,1,2)$-mixed Moore graph, then there exist sets $A, B \subseteq \mathrm{V}(G)$ such that the following properties hold.*

Property (i) $|A| = |B| = 9$*;*

Property (ii) $A \cap B = \emptyset$*;*

Property (iii) the subgraphs of G induced by A and B are composed of 3 disjoint directed 3-cycles.



Proof. As G is a $(3,1,2)$-mixed Moore graph, Lemma 3.3 tells us that G contains 6 directed 3-cycles. Let $U = \{u_1, u_2, u_3\}$ be one of these 3-cycles such that $u_1 \to u_2 \to u_3 \to u_1$. As each u_i has undirected degree 3, they have 3 more neighbours each. Let V_i be the set of undirected neighbours of each u_i. We must have that $V_i \cap V_j = \emptyset$ for all $i \neq j$, otherwise there would be a vertex v such that both $v \sim u_{i+1}$ and $v \sim u_i \to u_{i+1}$ for some i, contradicting 2-geodesity of G. Now, we have that u_1 is distance at most 2 from each vertex in V_3, which may only happen if there is some $v' \in V_1$ such that $v' \sim v$ or $v' \to v$. We cannot have $v' \sim v$ as then we would have $v \sim u_3 \to u_1$ and $v \sim v' \sim u_1$, contradicting 2-geodesity. By symmetry we now have that for each $v \in V_{i+1}$ there is some $v' \in V_i$ such that $v \to v'$.

Now let $V = \bigcup V_i$. Clearly the subgraph G_V of G induced by the vertices of V contains 3 directed 3-cycles. Further, if there were an undirected edge in V then we would contradict 2-geodesity as already shown. Hence V is composed of 3 disjoint directed 3-cycles.

Finally, let $W = \mathrm{V}(G) \setminus (U \cup V)$ be the set of the remaining vertices of G. As the diameter of G is 2, for any $w \in W$ we must have that $\mathrm{d}(w, u_i) = 2$ for each u_i. Therefore w must have neighbours in each V_i. These must be via undirected edges, as the directed in and out neighbours of each $v \in V$ are accounted for. Hence, all 3 of the undirected edges of w are adjacent to vertices in V. Letting $A = U \cup W$ we now see that the subgraph G_A of G induced by vertices of A contains no undirected edges. Further, it must contain 3 disjoint directed 3-cycles.

We finally prove the claim by taking $A = U \cup W$ and $B = V$. □

Now for an arbitrary $(3,1,2)$-mixed Moore graph G with some distinguished directed 3-cycle $U = \{u_1, u_2, u_3\}$ such that $u_1 \to u_2 \to u_3 \to u_1$, we may find sets with the properties of sets A and B of the previous lemma and label the vertices of G such that A is composed of directed 3-cycles A_1, A_2 and A_3, with $A_1 = U$, and B is composed of directed 3-cycles B_1, B_2 and B_3. We now have the following lemma.

Lemma 3.21. *For all $1 \leq i, j \leq 3$, the subgraph of G induced by the vertices of A_i and B_j is isomorphic to the $(1, 1, 2)$-mixed Moore graph.*

Proof. Without loss of generality we take $i = j = 1$, and let $A_1 = \{a_1, a_2, a_3\}$ such that $a_1 \to a_2 \to a_3 \to a_1$ and let $B_1 = \{b_1, b_2, b_3\}$ such that $b_1 \leftarrow b_2 \leftarrow b_3 \leftarrow b_1$. First we aim to show that there is some a_i and b_j such that $a_i \sim b_j$. As G is diameter 2, we must have $\mathrm{d}(a_i, b_j) \leq 2$ for each a_i and b_j. If $\mathrm{d}(a_i, b_j) = 1$ then we are done, hence assume $\mathrm{d}(a_i, b_j) = 2$. In this case there is some $v \in \mathrm{V}(G)$ such that a_i, v, b_j is a path in G. If v is in A, then we must have that $a_i \to v$ and $v = a_{i+1}$, giving that $a_{i+1} \sim b_j$ and we are done. Otherwise v is in B, and we have $v \to b_j$ and so $v = b_{j-1}$ and $a_i \sim b_{j-1}$ and we are done. Now without loss of generality we may take $i = j = 1$ and so in our labelling $a_1 \sim b_1$. Finally, from the fact $\mathrm{d}(a_1, b_2) \leq 2$ we deduce that $a_2 \sim b_2$ and from $\mathrm{d}(b_1, a_3) \leq 2$ we deduce $a_3 \sim b_3$. Therefore the subgraph of G induced by the vertices of A_i and B_j is isomorphic to the $(1, 1, 2)$-mixed Moore graph. □

With the vertices of G split into sets $A, B \subseteq \mathrm{V}(G)$ with the above properties, we now choose a labelling of the vertices of the graph G such that the following properties hold.

i) we label each $v \in A$ as $a_{i,j}$ for some $1 \leq i, j \leq 3$ such that $a_{i,j} = a_{i',j'}$ if, and only if, $i = i'$ and $j = j$;

ii) we label each $v \in B$ as $b_{i,j}$ for some $1 \leq i, j \leq 3$ such that $b_{i,j} = b_{i',j'}$ if, and only if, $i = i'$ and $j = j'$;

iii) we have $a_{i,1} \to a_{i,2} \to a_{i,3} \to a_{i,1}$ for each $1 \leq i \leq 3$;

iv) we have $b_{i,1} \leftarrow b_{i,2} \leftarrow b_{i,3} \leftarrow b_{i,1}$ for each $1 \leq i \leq 3$;

v) for each $1 \leq i, j \leq 3$ we have $a_{1,j} \sim b_{i,j}$;

vi) for each $1 \leq i, j \leq 3$ we have $b_{1,j} \sim a_{i,j}$.

Lemma 3.22. *A labelling of the vertices of G with the above properties exists.*

Proof. We have already shown the existence of the sets A and B in Lemma 3.20, and from the fact A and B are both composed of 3 disjoint directed 3-cycles it is trivial that we can choose a labelling satisfying properties (i), (ii), (iii) and (iv). Now we define the sets A_i and B_i such that $A_i = \{a_{i,1}, a_{i,2}, a_{i,3}\}$ and $B_i = \{b_{i,1}, b_{i,2}, b_{i,3}\}$. Now consider an arbitrary labelling of G satisfying properties (i), (ii), (iii) and (iv). From Lemma 3.21 we see that the subgraph of G induced by A_1 and B_i is the

$(1,1,2)$-Moore graph, and so if we have $a_{1,1} \sim b_{i,1+k}$ we have $a_{1,j} \sim b_{i,j+k}$. We may relabel $b_{i,j+k}$ to $b_{i,j}$, which preserves properties (i), (ii), (iii) and (iv) and now satisfies property (v). We finally repeat this step considering the subgraphs of G induced by B_1 and each A_i. □

We shall now continue this section with G as an arbitrary $(3,1,2)$-mixed Moore graph labelled as described above.

Lemma 3.23. *If $a_{i,j} \sim b_{i',j+k}$ for some i, i', j, k then $a_{i,j'} \sim b_{i',j'+k}$ for all $1 \leq j' \leq 3$. (Here we consider indices to wrap, e.g. 4 wraps to 1, 5 to 2 etc).*

Proof. For $i = 1$ or $i' = 1$ we have $k = 0$ and we are done. Otherwise, by assumption we have that $a_{i,j} \sim b_{i',j+k}$, and we have that $a_{i,1} \to a_{i,2} \to a_{i,3} \to a_{i,1}$ and $b_{i',1} \leftarrow b_{i',2} \leftarrow b_{i',3} \leftarrow b_{i',1}$. Further, we have that the subgraph of G induced by the vertices of A_i and $B_{i'}$ is the $(1,1,2)$-mixed Moore graph, from which the claim immediately follows. □

Corollary 3.24. *For each $1 \leq i, j \leq 3$ there exists some unique $0 \leq n \leq 2$ such that $a_{i,k} \sim b_{j,k+n}$ for $1 \leq k \leq 3$.*

As before, for a given pair i, j such that $1 \leq i, j \leq 3$ we shall call the n of Corollary 3.24 the *offset* of A_i and B_j. We shall again define the *offset matrix* of A and B as the matrix $M \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ such that $m_{i,j}$ is the offset of A_i and B_j.

Noting that $M \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ uniquely determines all edges of G outside of A and B, for an arbitrary $M \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ we shall denote by G_M the graph whose offset matrix is M. Note that for arbitrary M it is not necessarily the case that G_M is a $(3,1,2)$-mixed Moore graph.

So far what we have shown is that an arbitrary $(3,1,2)$-mixed Moore graph can have its vertices labelled such that its offset matrix M is of the form

$$M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & - & - \\ 0 & - & - \end{pmatrix}.$$

As before, we introduce an equivalence relation $\approx$ on matrices $M, N \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ which has the property that if $M \approx N$ then $G_M \cong G_N$. We define $\approx$ to be the transitive closure of the following.

i) $M \approx N$ for all $M, N \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ such that N can be formed by permuting the columns of M;

ii) $M \approx N$ for all $M, N \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ such that N can be formed by permuting the rows of M;

iii) $M \approx N$ for all $M, N \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ such that N can be formed by adding some $k \in \mathbb{Z}/3\mathbb{Z}$ to each entry in the first column of M;

iv) $M \approx N$ for all $M, N \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ such that N can be formed by adding some $k \in \mathbb{Z}/3\mathbb{Z}$ to each entry in the first row of M.

Lemma 3.25. *If $M \approx N$ then $G_M \cong G_N$.*

Proof. We first consider the case where $M, N \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ are related by one of the above rules.

If $M \approx N$ by rule (i), then letting $\pi \in S_3$ be the permutation of columns relating M to N we have that $\phi : G_M \to G_N$ given by $\phi(a_{i,j}) = a_{\pi(i),j}$ and $\phi(b_{i,j}) = b_{i,j}$ is an isomorphism from G_M to G_N.

The case $M \approx N$ by rule (ii) is symmetric to the previous case.

If $M \approx N$ by rule (iii), then letting $k \in \mathbb{Z}/3\mathbb{Z}$ be the number added to the first column of M to form N we have that the function $\phi : G_M \to G_N$ given by $\phi(a_{1,i}) = a_{1,i+k}$ for $1 \leq i \leq 3$ and $\phi(v) = v$ for all $v \in \mathrm{V}(G) \setminus A_1$ is an isomorphism from G_M to G_N.

The case where $M \approx N$ by rule (iv) is symmetric to the previous case.

Finally, for $M \approx N$ as a result of a combination of these rules the fact $G_M \cong G_N$ follows from a trivial induction and the fact that the property of being isomorphic is transitive. □

We again require a technical lemma to help us reduce the search space for potential offset matrices of $(3, 1, 2)$-mixed Moore graphs.

Lemma 3.26. *If M is an offset matrix such that G_M is a $(3, 1, 2)$-mixed Moore graph then for any $x, y, i, j \in \mathbb{Z}/3\mathbb{Z}$ such that $x \neq y$ and $i \neq j$ we have $m_{x,i} - m_{y,i} \neq m_{x,j} - m_{y,j}$.*

Proof. We first create a matrix N such that $M \approx N$ by performing the following transformations on M.

i permute the columns of M by some permutation $\pi \in S_3$ such that $\pi(x) = 1$ and $\pi(y) = 2$;

ii permute the rows of M by some permutation $\pi \in S_3$ such that $\pi(i) = 1$ and $\pi(j) = 2$;

iii add $-m_{x,i}$ to column 1 and $-m_{x,j}$ to column 2;

iv add $-(m_{y,i} - m_{x,i})$ to row 2.

We illustrate the transformation with the following example.

$$M = \begin{pmatrix} - & - & - \\ - & m_{x,i} & m_{x,j} \\ - & m_{y,i} & m_{y,j} \end{pmatrix} \xrightarrow{i} \begin{pmatrix} - & - & - \\ m_{x,i} & m_{x,j} & - \\ m_{y,i} & m_{y,j} & - \end{pmatrix} \xrightarrow{ii} \begin{pmatrix} m_{x,i} & m_{x,j} & - \\ m_{y,i} & m_{y,j} & - \\ - & - & - \end{pmatrix}$$
$$\xrightarrow{iii} \begin{pmatrix} 0 & 0 & - \\ m_{y,i} - m_{x,i} & m_{y,j} - m_{x,j} & - \\ - & - & - \end{pmatrix} \xrightarrow{iv} \begin{pmatrix} 0 & 0 & - \\ 0 & (m_{x,i} - m_{y,i}) - (m_{x,j} - m_{y,j}) & - \\ - & - & - \end{pmatrix}.$$

Now, if $m_{x,i} - m_{y,i} = m_{x,j} - m_{y,j}$ then we have

$$N = \begin{pmatrix} 0 & 0 & - \\ 0 & 0 & - \\ - & - & - \end{pmatrix}.$$

Therefore in the graph G_N there exists the 4-cycle $a_{1,1} \sim b_{2,1} \sim a_{2,1} \sim b_{1,1} \sim a_{1,1}$, contradicting 2-geodesity of G_N, so we cannot have that $m_{x,i} - m_{y,i} = m_{x,j} - m_{y,j}$. □

We are now in a position to prove our first important result about $(3, 1, 2)$-mixed Moore graphs.

Proposition 3.27. *There is a unique* $(3, 1, 2)$*-mixed Moore graph up to isomorphism.*

Proof. Let G be a $(3, 1, 2)$-mixed Moore graph. From Lemma 3.22 we may label the vertices of G such that G is described by an offset matrix $M \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ of the form,

$$M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix},$$

for some $a, b, c, d \in \mathbb{Z}/3\mathbb{Z}$. Applying Lemma 3.26 we have that $a, b \neq 0$ and $a \neq b$. As $a, b \in \mathbb{Z}/3\mathbb{Z}$ this gives us the possibilities $a = 1$ and $b = 2$ or $b = 1$ and $a = 2$. If $a = 1$

and $b = 2$ then by Lemma 3.26 we have that $c = 2$ and $d = 1$. Otherwise, if $a = 2$ and $b = 1$ then by Lemma 3.26 we have that $c = 1$ and $d = 2$. Hence we have that G is isomorphic to either G_N or $G_{N'}$ where N and N' are given by

$$N = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix} \quad \text{and} \quad N' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Finally, we note that $N \approx N'$ by permutation of columns, and so $G_N \cong G_{N'}$ by Lemma 3.25. Hence we have $G \cong G_N$ for any $(3, 1, 2)$-mixed Moore graph G. □

We have now replicated the proof of Proposition 3.16 for the case of the Bosák graph. Our proofs have closely matched one another, showing the fundamental similarities between these two cases. Further, as before, we can now go on to derive properties of the automorphism group of the Bosák graph in the same manner as for the Hoffman-Singleton graph.

For the rest of this section we shall refer to the unique $(3, 1, 2)$-mixed Moore graph as the Bosák graph and denote it by G.

Lemma 3.28. *For each directed 3-cycle $U = \{u_1, u_2, u_3\} \subseteq \mathrm{V}(G)$ such that $u_1 \to u_2 \to u_3 \to u_1$, and each vertex $v \in \mathrm{V}(G)$ such that $\mathrm{d}(v, u_i) = 2$ for each u_i, there is at most one automorphism $\phi \in \mathrm{Aut}(G)$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$.*

Proof. Suppose that $\phi \in \mathrm{Aut}(G)$ is an automorphism with these properties. Considering the paths from v to each u_i, as $\mathrm{d}(v, u_i) = 2$ there is a uniquely defined $w_i \in \mathrm{V}(G)$ such that v, w_i, u_i is a path. As $\phi(v) = a_{2,1}$ and $\phi(u_i) = a_{1,i}$, we know that the unique paths of length 2 from $a_{2,1}$ to each $a_{1,i}$ go via $b_{i,i}$. Hence, we must have that $\phi(w_i) = b_{i,i}$ for each $1 \leq i \leq 3$. Now, as each $b_{i,i}$ has unique directed in and out neighbours, namely $b_{i,i+1}$ and $b_{i,i-1}$ respectively, we must have that the directed in and out neighbours of each w_i map to $b_{i,i+1}$ and $b_{i,i-1}$ respectively. Therefore, from the information that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$ we have determined the pre-image of ϕ of each vertex in B. By symmetry, we now may determine the pre-image of ϕ of each vertex in A. Altogether we see that ϕ is uniquely determined. □

Lemma 3.29. *For each directed 3-cycle $U = \{u_1, u_2, u_3\} \subseteq \mathrm{V}(G)$ such that $u_1 \to u_2 \to u_3 \to u_1$, and each vertex $v \in \mathrm{V}(G)$ such that $\mathrm{d}(v, u_i) = 2$ for each u_i, there is at least one automorphism $\phi \in \mathrm{Aut}(G)$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$.*

Proof. We consider finding a relabelling of $\mathrm{V}(G)$ into sets A, B with the usual properties such that $u_i = a_{1,i}$ and $v = a_{2,1}$. Clearly that is equivalent to finding the

desired automorphism. First, from the derivation of Lemma 3.20 it is clear that for an arbitrary directed 3-cycle $U \subseteq \mathrm{V}(G)$ we can find sets $A, B \subseteq \mathrm{V}(G)$ such that A and B have the desired properties and $U \subseteq A$. Now, we may label the vertices in A as $a_{i,j}$ and the vertices in B as $b_{i,j}$ such that we have properties (i), (ii, (iii) and (iv) in our labelling. In addition, we may choose to do this in such a way that $u_i = a_{1,i}$ and $v = a_{2,1}$. This now gives some labelling of G which implies some offset matrix $M \in \mathbb{M}^3(\mathbb{Z}/3\mathbb{Z})$ and an isomorphism $\phi : G \to G_M$ such that $\phi(u_i) = a_{1,i}$ and $\phi(v) = a_{2,1}$.

We now aim to find a matrix N such that $M \approx N$ so that we have an isomorphism $\psi : G_M \to G_N$ in which $\psi(a_{1,i}) = a_{1,i}$ and $\psi(a_{2,1}) = a_{2,1}$ and N is given by

$$N = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}.$$

Hence, we apply the following transformations to G_M.

i) add constants to each row of M so that the first entry of each row is 0;

ii) permute the rows of M' such that the second entry of each row is in ascending order;

iii) add a constant to the third column of M'' such that the first entry of the third column is 0.

We illustrate these transformations as follows.

$$M = \begin{pmatrix} c_1 & - & - \\ c_2 & - & - \\ c_3 & - & - \end{pmatrix} \xrightarrow{i} \begin{pmatrix} 0 & d_1 & - \\ 0 & d_2 & - \\ 0 & d_3 & - \end{pmatrix} \xrightarrow{ii} \begin{pmatrix} 0 & 0 & e \\ 0 & 1 & - \\ 0 & 2 & - \end{pmatrix} \xrightarrow{iii} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & f_1 \\ 0 & 2 & f_2 \end{pmatrix}.$$

We note that d_1, d_2 and d_3 are guaranteed to be distinct by Lemma 3.26. We also note as we didn't either permute the columns of M nor add any constants to the first two columns the implied isomorphism $\psi : G_M \to G_N$ has the property $\psi(a_{1,i}) = a_{1,i}$ and $\psi(a_{2,1}) = a_{2,1}$. Finally, from Lemma 3.26 we see that $f_1 = 2$ and $f_2 = 1$, and that G_N is the standard labelling of the Bosák graph. Hence, we have found an automorphism $\theta = \phi \circ \psi$ such that $\theta(u_i) = a_{1,i}$ and $\theta(v) = a_{2,1}$ for an arbitrary directed 3-cycle U and vertex v at distance 2 from U in the Bosák graph. □

We are now in a position to give our final result concerning the automorphisms of the Bosák graph.

Proposition 3.30. *We have the following facts about the automorphisms of the Bosák graph.*

i) The automorphisms of the Bosák graph are uniquely characterised by their action on a directed 3-cycle and a single vertex at distance 2 from all points in the cycle.

ii) There are 108 automorphisms of the Bosák graph.

iii) The Bosák graph is vertex transitive.

Proof. The characterisation of the automorphism group of the Bosák graph follows immediately from Lemma 3.28 and Lemma 3.29. The fact that the Bosák graph is vertex transitive follows from the fact every vertex is in a directed 3-cycle and Lemma 3.29. Finally, we count the automorphism by noting there are 6 directed 3-cycles in the Bosák graph, each of which can be chosen in one of 3 orientations to be our choice of directed 3-cycle U, and that there are then 6 possible choices of the vertex v at distance 2 from all vertices in U. This gives $6 \times 3 \times 6 = 108$ automorphisms of the Bosák graph. □

3.5 Other Possible Cases

Following from what we have seen it is natural to ask if the construction we have used for the Hoffman-Singleton graph and the Bosák graph can be generalised to other new cases. In this section we generalise the structure from the previous sections and show that the Petersen graph, Hoffman-Singleton graph, $(1, 1, 2)$-mixed Moore graph and Bosák graph are the only graphs which have this particular structure.

First we note that in the case of the Hoffman-Singleton graph and the Bosák graph we split the graphs into bipartitions of 5-cycles and directed 3-cycles respectively. In particular, we have found some bipartition of the vertices into sets A and B such that the subgraphs induced by the vertices of A and B are composed of multiple copies of either the 5-cycle or the directed 3-cycle. Then, all subsequent edges of the graph are undirected and connect vertices from A to vertices in B.

We shall generalise this idea in the following way. In both cases we notice that the 5-cycle and directed 3-cycle are mixed Moore graphs. Hence, we shall consider any mixed Moore graph G and two sets of vertices $A, B \subseteq \mathrm{V}(G)$ such that the following properties hold.

i) $A \cap B = \emptyset$;

ii) $A \cup B = \mathrm{V}(G)$;

iii) there is some mixed Moore graph H and some number n such that the subgraphs of G induced by A and B are isomorphic to n disjoint copies of H.

We note that we allow the special case $n = 1$, so that the Petersen graph and the $(1, 1, 2)$-mixed Moore graph also fit this generalisation. We now aim to show that the only mixed Moore graphs for which sets A and B exist with the above properties are the Petersen graph, Hoffman-Singleton graph, $(1, 1, 3)$-mixed Moore graph and Bosák graph.

For the rest of this section, let G and H be mixed Moore graphs and $A, B \subseteq \mathrm{V}(G)$ with the above properties. Further, let $A = A_1 \cup A_2 \cup \cdots \cup A_n$ and $B = B_1 \cup B_2 \cup \cdots \cup B_n$ where $A_i \cap A_j = B_i \cap B_j = \emptyset$ for all $i \neq j$ and the subgraph of G induced by each A_i or B_i is isomorphic to H.

Lemma 3.31. *The subgraph $G_{i,j}$ of G induced by the vertices $A_i \cup B_j$ for any $1 \leq i, j \leq n$ is a mixed Moore graph.*

Proof. By assumption we already have that the subgraphs of G induced by A_i and B_j are mixed Moore graphs. Hence, in the subgraph of G induced by $A_i \cup B_j$ we need only consider how long paths are which connected vertices from A_i to B_j and vice versa. Let $u \in A_i$ and $v \in B_j$, as G is an $(r, z, 2)$-mixed Moore graph we have that $\mathrm{d}(u, v) \leq 2$. We consider the following cases. First, if $\mathrm{d}(u, v) = 1$ then we have that $u \sim v$ and so $\mathrm{d}(u, v) = 1$ in $G_{i,j}$. Otherwise, we have $\mathrm{d}(u, v) = 2$, and there is some vertex $w \in \mathrm{V}(G)$ such that $u \sim w \sim v$. If $w \in A$, then we must have $w \in A_i$ as $u \sim w$ and $u \in A_i$, so the path $u \sim w \sim v$ is in $G_{i,j}$ and we have $\mathrm{d}(u, v) = 2$ in $G_{i,j}$. Otherwise, we must have $w \in B$, and so $w \in B_j$ as $w \sim v$, again giving that the path $u \sim w \sim v$ is in $G_{i,j}$ and that $\mathrm{d}(u, v) = 2$ in $G_{i,j}$.

Hence we have shown that the graph $G_{i,j}$ is diameter 2. Finally, it follows that $G_{i,j}$ is 2-geodetic as $G_{i,j}$ is the subgraph of an $(r, z, 2)$-mixed Moore graph. The combination of being diameter 2 and 2-geodetic means that $G_{i,j}$ is a mixed Moore graph. □

We now let K be the subgraph of G induced by A_1 and B_1.

Lemma 3.32. *If H is an $(r, z, 2)$-mixed Moore graph, then K is an $(r + 1, z, 2)$-mixed Moore graph.*

Proof. As K is a mixed Moore graph we have that K is totally regular. Hence we may define r' and z' such that K is an $(r', z', 2)$-mixed Moore graph. Further, we have that

there are sets $A, B \subseteq \mathrm{V}(K)$ such that the subgraphs of K induced by A and B are isomorphic to H and A and B are disjoint. For an arbitrary vertex $u \in \mathrm{V}(G)$ we have that if $u \in A$ then u has r undirected neighbours in A and z directed neighbours in A, the case for B being symmetric. This shows that $r' \geq r$ and $z' \geq z$. Further, we must have that, for an arbitrary vertex $u \in A$, u has $r' - r$ undirected neighbours in B and $z' - z$ directed neighbours in B (with the case for A and B being reversed symmetric).

Now, assume that $z' > z$. We pick an arbitrary vertex $u \in A$, as $z' > z$ we have that u has at least one directed neighbour v in B, and again as $z' > z$ we have that v has at least one directed neighbour w in A. Hence, as K restricted to A is a mixed Moore graph there is a path of length at most 2 from u to w via vertices in A, but we also have the path $u \to v \to w$, so K cannot be 2-geodetic, contradicting that K is a mixed Moore graph. Therefore we cannot have $z' > z$ and so $z' = z$.

Given that $z' = z$ we clearly must have $r' > r$ otherwise K is not connected. Hence assume that $r' \geq r + 2$. If this is the case, then again for some vertex $u \in A$ we have that u has some undirected neighbour $v \in B$, and that v has some directed neighbour $w \in A$ such that $w \neq u$. Now, we have that u and w are connected by a path of length at most 2 via vertices only in A, as K restricted to A is a mixed Moore graph. However, we also have that $u \sim v \sim w$ is a different path of length at most 2 from u to w in K, contradicting that K is 2-geodetic. Therefore, we cannot have $r' \geq r + 2$, and as $r' > r$ we must therefore have $r' = r + 1$. □

We now find restrictions on the parameters r and z of the mixed Moore graph H.

Lemma 3.33. *With the given above definitions, we must have* $r + z = (r + z)^2 - r$.

Proof. Let K, A, B be defined as above. We consider the paths from vertices in A to vertices in B. We have that each $u \in A$ has one neighbour v in B and $(r + z)$ neighbours v_i in A; the vertex v has $(r + z)$ neighbours w_i in B; and the vertices v_i have one neighbour x_i each in B. These are all the possible paths of length at most 2 to the vertices of B from the vertex u, and as K is an $(r + 1, z, 2)$-mixed Moore graph these must be all of the vertices in B. Hence $B = \{v\} \cup \{w_i\} \cup \{x_i\}$, giving that $|B| = 1 + (r + z) + (r + z)$. Alternately, we may count the vertices of B from the fact the subgraph of K induced by B is isomorphic to H, an $(r, z, 2)$-mixed Moore graph, and so has $1 + (r + z) + r(r - 1 + z) + z(r + z)$ vertices. Therefore we have $1 + 2(r + z) = 1 + (r + z) + (r + z)^2 - r$, giving the claim. □

Corollary 3.34. *Either* $r = 2$ *and* $z = 0$ *or* $r = 0$ *and* $z = 1$.

Proof. From the equation $(r+z) = (r+z)^2 - r$ we have that $-r \equiv 0 \pmod{r+z}$. As $r, z \geq 0$ we therefore either have $r = 0$ or $z = 0$. If $r = 0$ then the equation becomes $z = z^2$, i.e. $z(z-1) = 0$ which has solutions $z = 0$ or $z = 1$, giving the solution $r = 0$ and $z = 1$. Otherwise, if $z = 0$ then the equation becomes $r = r^2 - r$, i.e. $r(r-2) = 0$ which has solutions $r = 0$ and $r = 2$, giving the solution $r = 2$ and $z = 0$. □

We are now in a position to give our first important result.

Proposition 3.35. *With the above definitions, we either have H is a 5-cycle or H is a directed 3-cycle.*

Proof. The graph H is an $(r, z, 2)$-mixed Moore graph. From the above work this gives two possibilities. First, for $r = 2$ and $z = 0$ we have that H is a $(2, 0, 2)$-mixed Moore graph, which is a 5-cycle. Second, for $r = 0$ and $z = 1$ we have that H is a $(0, 1, 2)$-mixed Moore graph, which is a directed 3-cycle. □

We have now put in the work to show that the only possibilities for the subgraph H of G is the 5-cycle or the directed 3-cycle. Now we shall conclude by showing that the only graphs built from bipartitions of said subgraphs are those listed above.

In the following, let G be an $(r', z, 2)$-mixed Moore graph with bipartitions $A = A_1 \cup A_2 \cup \cdots \cup A_n$ and $B = B_1 \cup B_2 \cup \cdots \cup B_n$ as before where each subgraph induced by A_i or B_i is isomorphic to an $(r, z, 2)$-mixed Moore graph H.

Lemma 3.36. *With the above definitions, $r' = r + n$.*

Proof. As we have shown, the subgraphs of G induced by any A_i and B_j are $(r+1, z, 2)$-mixed Moore graphs, hence for an arbitrary $u \in A_1$ we see that u has exactly one undirected neighbour in each B_i, and by assumption we know all of the neighbours of u in A are in A_1, so u has $r + n$ undirected neighbours and z directed neighbours. The result follows immediately as G is a mixed Moore graph and, therefore, totally regular. □

Lemma 3.37. *Either $n = 1$ or $n = |\operatorname{V}(H)|$.*

Proof. We must have $n \geq 1$. The cases of the Petersen graph and $(1, 1, 2)$-mixed Moore graph show that we may have $n = 1$, so we now consider the case $n > 1$. In this case, consider a vertex $u \in A_1$. We must have that u is distance at most 2 from all the vertices in $A \setminus A_1$, and we clearly have $|A \setminus A_1| = (n-1)|\operatorname{V}(H)|$. For any $v \in A \setminus A_1$ we know that u and v are not adjacent by assumption, so we must have

$\mathrm{d}(u, v) = 2$ and there is some $w \in B$ such that $u \sim w \sim v$. Conversely, we know that u has n neighbours $w_i \in B$, and each w_i has 1 neighbour in A_1, which is u, and $n-1$ neighbours in $A \setminus A_1$, say $v_{i,j}$. By 2-geodesity we must have $\{v_{i,j} | 1 \leq i \leq n, 1 \leq j < n\} \subseteq A \setminus A_1$, so we have $|A \setminus A_1| \geq n(n-1)$. Further, these are all possible paths from A_1 to $A \setminus A_1$, so we must have $|A \setminus A_1| = n(n-1)$. Hence we have $n(n-1) = (n-1)|\mathrm{V}(H)|$, from which the result immediately follows. □

Proposition 3.38. *The only mixed Moore graphs of diameter 2 which can be split into bipartitions of disjoint pairwise isomorphic mixed Moore graphs of diameter 2 are*

i) the Petersen graph;

ii) the Hoffman-Singleton graph;

iii) the unique $(1, 1, 2)$*-mixed Moore graph;*

iv) the Bosák graph.

Proof. From Proposition 3.35 we need only consider the case of H as a 5-cycle or a directed 3-cycle, and from Lemma 3.37 we need only consider the cases $n = 1$ or $n = |\mathrm{V}(H)|$. This gives us the following four cases.

i) For H is a 5-cycle and $n = 1$ we have that G is the Petersen graph.

ii) For H is a 5-cycle and $n = |\mathrm{V}(H)| = 5$ we have that G is the Hoffman-Singleton graph.

iii) For H is a directed 3-cycle and $n = 1$ we have that G is the unique $(1, 1, 2)$-mixed Moore graph.

iv) For H is a directed 3-cycle and $n = 3$ we have that G is the Bosák graph.

□

3.6 Conclusion

Altogether in this section we have derived the Hoffman-Singleton and Bosák graphs from first principles, showing their shared structure and deriving their shared property of vertex-transitivity. We have also shown that these are the only two mixed Moore graphs for any parameters that have this shared structure.

We now note that a standard algebraic argument shows that the only possible parameters for which there can exist an $(r, 0, 2)$-mixed Moore graph are $r = 2, 3, 7$ or

57, with $r = 2$ corresponding to the 5-cycle, $r = 3$ corresponding to the Petersen graph, $r = 7$ corresponding to the Hoffman-Singleton graph and $r = 57$ corresponding to the unknown case of a possible $(57, 2)$-Moore graph. Similarly, an analogous algebraic argument shows that the only possible parameters for which there can exist an $(r, 1, 2)$-mixed Moore graph are $r = 0, 1, 3$ or 21, with $r = 0$ corresponding to the directed 3-cycle, $r = 1$ corresponding to the unique $(1, 1, 2)$-mixed Moore graph, $r = 3$ corresponding to the Bosák graph, and $r = 21$ corresponding to the unknown case of a possible $(21, 1, 2)$-mixed Moore graph.

Hence, we may conclude a similarity between the famous unknown case of a possible $(57, 2)$-Moore graph and that of a potential $(21, 1, 2)$-mixed Moore graph. In particular, the case of a possible $(21, 1, 2)$-mixed Moore graph represents a smaller graph, and so it is likely a more approachable problem, suggesting that progress towards resolving the problem of whether a $(21, 1, 2)$-mixed Moore graph exists is both more approachable than a $(57, 2)$-Moore graph and could provide insight into how to approach the latter case.

In addition to this similarity, we may also consider the implications of our observations to other mixed Moore graphs. The other known non-trivial mixed Moore graphs are the Kautz digraphs $\mathrm{Ka}(n, 2)$ for $n \geq 2$ and the mixed Moore graphs of Jørgensen presented in [35]. From the work we have done in this section we see that to understand their structure as being derived from smaller mixed Moore graphs ideas of a different nature are required.

Chapter 4

Word Graphs

4.1 Introduction

Before we begin our own work on word graphs, we begin by giving motivating examples of word graphs. These examples are the Faber-Moore-Chen and Gómez graphs. We will then provide a natural generalisation of these two families of graphs which we call word graphs. We then derive results about word graphs and apply them to the case of Gómez graphs. We first show that the Gómez graphs are the largest graphs for given degree and diameter within our generalisation, and we subsequently show that Gómez graphs are not Cayley graphs in general, a previously unknown result about Gómez graphs.

4.2 Faber-Moore-Chen Digraphs

The Faber-Moore-Chen digraphs were introduced by Faber, Moore and Chen in [24, 25] and further studied by Comellas and Fiol in [12]. We define them as follows.

Let X be a set of $n = d - k$ distinct symbols. The Faber-Moore-Chen graph $\mathrm{FMC}(d, k)$ has the vertex set

$$\mathrm{V}(\mathrm{FMC}(d,k)) = \{x_1 x_2 \dots x_k | x_i \in X, x_i \neq x_j\}. \tag{4.1}$$

i.e. the vertices of the Faber-Moore-Chen digraphs are tuples or *words* of length k made up from distinct elements of the set X. An arbitrary vertex $x_1 x_2 \dots x_k$ of a Faber-Moore-Chen digraph has the following adjacencies:

i) $x_1 x_2 \dots x_k \to x_2 x_3 \dots x_k y$ for each $y \in X \setminus \{x_1, x_2, \dots, x_k\}$.

ii) $x_1 x_2 \dots x_k \to x_2 x_3 \dots x_i x_1 x_{i+1} \dots x_k$ for each $1 < i \leq k$.

i.e. either we can introduce a new letter not present in the word at the end, or we can cycle a prefix of the word of any length (hence the Faber-Moore-Chen digraphs are also known as *cycle prefix digraphs*).

The Faber-Moore-Chen digraphs are interesting because they are asymptotically close

to the Moore bound. To show this, we must count the vertices of $\mathrm{FMC}(d,k)$ and show that the diameter of $\mathrm{FMC}(d,k)$ is at most k.

Proposition 4.1. *The graph* $\mathrm{FMC}(d,k)$ *has* $n!/(n-k)! \sim d^k$ *vertices for fixed* k *and* $d \to \infty$.

Proof. Each vertex is an ordered set of k distinct symbols from a set of n possible symbols. Therefore we have $|\,\mathrm{V}(\mathrm{FMC}(d,k))| = \binom{n}{k}k! = n!/(n-k)!$. As $n = (d-k)$ we have $|\,\mathrm{V}(\mathrm{FMC}(d,k))| = (d-k)!/(d-2k)! = (d-k)(d-k-1)\dots(d-2k+1) \sim d^k$. □

Proposition 4.2. *The graph* $G = \mathrm{FMC}(d,k)$ *has diameter at most* k.

Proof. We show this result by constructing a path of length k from an arbitrary start vertex $x = x_1x_2\dots x_k$ to an arbitrary destination vertex $y = y_1y_2\dots y_k$. We relabel the elements of the alphabet X to be the set $\{1,2,\dots,n\}$ in any way such that $y = 1\ 2\ \dots\ k$. We now construct a path $z^0 = x \to z^1 \to \dots \to z^k = y$ from x to y as follows. The path we construct shall have two properties maintained at each step:

Property i) the last i letters of each z^i shall be from the set $\{1,2,\dots,k\}$ and sorted in ascending order;

Property ii) at each step z^i there is no $\alpha \in \{1,2,\dots,k\}$ such that $\alpha \notin z^i$ and $\alpha < z^i_{k-j}$ for any $0 \le j < i$ (i.e. there is no α smaller than any elements in the sorted part of z^i which is not in z^i).

This is trivially guaranteed to be true at z^0, and if it is true at z^k then $z^k = y$. In order to move from z^i to z^{i+1} we choose a rule as follows:

Rule i) if there is some $\alpha \in \{1,2,\dots,k\}$ such that $\alpha \notin z^i$ and $\alpha < z^i_0$, then we move from z^i to z^{i+1} using the rule $z^i_0z^i_1\dots z^i_k \to z^i_1z^i_2\dots z^i_k\alpha$,

Rule ii) otherwise we choose the rule that moves z^i_0 into its correct sorted position in the sorted part of z^{i+1}.

It is trivial that rule (ii) maintains property (i), and from property (ii) we also clearly see that rule (i) also maintains property (i). In the case of applying rule (ii) we see that as $z^i_0 < \alpha$ for all $\alpha \in \{1,2,\dots,k\}$ and $\alpha \notin z^i$ we maintain property (ii). Finally, in the case of applying rule (i) we see that property (ii) must be maintained as we choose the smallest possible α. Therefore at each stage we maintain both properties and from the definition of our rules we see we may always apply either rule (i) or rule (ii), and so our path from x to y is a well defined path of length k. □

4.3 Gómez Digraphs

The Gómez digraphs were introduced by Gómez in [29]. Similarly to the Faber-Moore-Chen digraphs we define them here as follows.

Let X be a set of $n = d - \lfloor k/2 \rfloor$ distinct symbols. The Gómez graph $\mathrm{GG}(d,k)$ has the vertex set

$$\mathrm{V}(\mathrm{GG}(d,k)) = \{x_1x_2\dots x_k | x_i \in X, x_i \neq x_j\}. \tag{4.2}$$

The adjacencies of the Gómez graphs are given as follows:

i) $x_1x_2\dots x_k \to x_2x_3\dots x_ky$ for each $y \in X \setminus \{x_1, x_2, \dots, x_k\}$.

ii) $x_1x_2\dots x_k \to x_2x_3\dots x_ix_1x_{i+2}x_{i+3}\dots x_kx_{i+1}$ for each $1 \leq i \leq k/2$.

That is, the adjacencies of a word either introduce a new symbol at the end of the word or split the word into two sub words and cycle both subwords. For example, if we take $X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ then the vertex $x_1x_2x_3x_4x_5$ has the following neighbours in $\mathrm{GG}(4,5)$

i) $x_1x_2x_3x_4x_5 \to x_2x_3x_4x_5x_6$;

ii) $x_1x_2x_3x_4x_5 \to x_2x_3x_4x_5x_7$;

iii) $x_1x_2x_3x_4x_5 \to x_1x_3x_4x_5x_2$;

iv) $x_1x_2x_3x_4x_5 \to x_2x_1x_4x_5x_3$.

Again, we show that the Gómez graphs are asymptotically close to the Moore bound analogously to how we did for the Faber-Moore-Chen graphs.

Proposition 4.3. *The graph* $\mathrm{GG}(d,k)$ *has* $n!/(n-k) \sim d^k$ *vertices for fixed* k *and* $d \to \infty$.

Proof. We immediately have $|\mathrm{V}(\mathrm{GG}(d,k))| = \binom{n}{k}k! = n!/(n-k)!$. Letting $m = \lfloor k/2 \rfloor$ we have $n = d - m$ and hence
$n!/(n-k)! = (d-m)!/(d-m-k)! = (d-m)(d-m-1)\dots(d-m-(k-1)) \sim d^k$. □

As with the Faber-Moore-Chen graphs, one may prove that the Gómez graphs are of diameter at most k. However, the proof is much more involved for the Gómez graphs, so we refer to [29] for the proof.

4.4 Word Graphs Definition

We begin by providing a natural generalisation for studying graphs like the Gómez graphs and the Faber-Moore-Chen graphs. The following definitions of word graphs are work of the author.

We choose a number k which will be the *word length*; some set $\Pi_k \subseteq S_k$, where S_k is the symmetric group, which will be the *rules*; and a number $n > k$ which shall be the *alphabet size*. We define the *word graph* $\mathrm{WG}(\Pi_k, n)$ as follows. Fix some arbitrary set B such that $|B| = n$, B shall be called the *alphabet* of $\mathrm{WG}(\Pi_k, n)$. The vertices of $\mathrm{WG}(\Pi_k, n)$ are given by $\mathrm{V}(\mathrm{WG}(\Pi_k, n)) = \{x_1x_2 \dots x_k | x_i \in B, x_i = x_j \Leftrightarrow i = j\}$, that is the vertices of $\mathrm{WG}(\Pi_k, n)$ are all words of length k all of whose letters are distinct. We form the directed adjacencies of an arbitrary word $x_1x_2 \dots x_k \in \mathrm{V}(\mathrm{WG}(\Pi_k, n))$ by the following rules

$$x_1x_2 \dots x_k \to \begin{cases} x_2x_3 \dots x_k y, & y \in B \setminus \{x_1, x_2, \dots, x_k\} \\ x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(k)}, & \pi \in \Pi_k. \end{cases}$$

We shall refer to the rules of the form $x_1x_2 \dots x_k \to x_2x_3 \dots x_k y$ as *alphabet changing* rules and rules of the form $x_1x_2 \dots x_k \to x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(k)}$ as *alphabet fixing* rules. For a vertex $x = x_1x_2 \dots x_k$ we define $\alpha : \mathrm{V}(\mathrm{WG}(\Pi_k, n)) \to B$ by $\alpha(x) = \{x_1, x_2, \dots, x_k\}$ and call $\alpha(x)$ the *alphabet* of x.

For a given Π_k we shall also denote by $\mathrm{WGF}(\Pi_k)$ the set of graphs $\{\mathrm{WG}(\Pi_k, k+1), \mathrm{WG}(\Pi_k, k+2), \mathrm{WG}(\Pi_k, k+2), \dots\}$. We shall call this the *word graph family* of Π_k.

We can express the Faber-Moore-Chen graphs and the Gómez graphs as word graphs as follows.

i) The Faber-Moore-Chen graphs are word graphs where we take $\Pi_k = \{(1\ 2), (1\ 2\ 3), \dots, (1\ 2\ \dots\ k)\}$,

ii) The Gómez graphs are word graphs where we take

$$\begin{aligned}\Pi_k = \{&(1\ 2\ \ldots\ k),\\ &(2\ 3\ \ldots\ k),\\ &(1\ 2)(3\ 4\ \ldots\ k),\\ &(1\ 2\ 3)(4\ 5\ \ldots\ k),\\ &\ldots,\\ &(1\ 2\ \ldots\ \lfloor k/2\rfloor)((\lfloor k/2\rfloor+1)\ (\lfloor k/2\rfloor+2)\ \ldots\ k)\},\end{aligned}$$

4.5 Basic Properties

As we are interested in word graphs from the point of view of the degree-diameter problem, we begin by studying the diameters of word graph families. We begin by considering a fixed rule set Π_k and the associated word graph family $\mathrm{WGF}(\Pi_k) = \{\mathrm{WG}(\Pi_k, k+1), \mathrm{WG}(\Pi_k, k+2), \ldots\}$. For brevity we shall use G_n to denote $\mathrm{WG}(\Pi_k, n)$.

We begin with some lemmas concerning the diameter of G_n as n is varied.

Lemma 4.4. *The degree of* $\mathrm{WG}(\Pi_k, n)$ *is* $n - k + |\Pi_k|$.

Proof. From an arbitrary vertex $x = x_1x_2\ldots x_k \in \mathrm{WG}(\Pi_k, n)$ there are $n-k$ alphabet changing rules giving adjacencies of x and $|\Pi_k|$ alphabet fixing rules giving adjacencies of x. □

Lemma 4.5. *For all* $n \geq 2k$ *we have* $\mathrm{Diam}(G_n) \geq k$.

Proof. Letting $\{x_1, x_2, \ldots x_k, y_1, y_2, \ldots y_k\} \subseteq B$, such that all x_i and y_j are distinct, we consider any path from the vertex $x = x_1x_2\ldots x_k$ to $y = y_1y_2\ldots y_k$. Let $z_0 = x \to z_1 \to \cdots \to z_m = y$ be such a path. Trivially, we have $|\alpha(z_0) \cap \alpha(z_m)| = 0$, and $|\alpha(z_{i+1}) \cap \alpha(z_m)| \leq |\alpha(z_i) \cap \alpha(z_m)| + 1$. Hence, as $|\alpha(z_m)| = k$ a trivial induction shows there must be at least k steps in a path from x to y. □

Lemma 4.6. *For all* $n \geq 3k$ *we have* $\mathrm{Diam}(G_n) \leq 2k$.

Proof. Consider arbitrary $x = x_1x_2\ldots x_k$ and $y = y_1y_2\ldots y_k$ in $\mathrm{V}(G_n)$. As $n \geq 3k$, we know that $|B \setminus (\alpha(x) \cup \alpha(y)| \geq k$, hence let $\{z_1, z_2, \ldots, z_k\} \subseteq B \setminus (\alpha(x) \cup \alpha(y))$. Now by using only alphabet changing rules we may form a path from x to y where in the first k steps we append z_i and in the second k steps we append y_i. This gives a path of length $2k$ connecting x and y. □

Lemma 4.7. *For all $n \geq 4k$ we have* $\mathrm{Diam}(G_n) = \mathrm{Diam}(G_{4k})$.

Proof. Let x and y be arbitrary vertices of G_n. Let $z_0 = x \to z_1 \to \cdots \to z_m = y$ be a shortest path connecting x and y. From Lemma 4.6 we know that a shortest path connecting x and y is at most length $2k$, so $m \leq 2k$. We now consider $B' = \bigcup_{i=0}^{2k} \alpha(z_i)$. As each z_{i+1} may introduce at most one letter not in z_i, and there are at most $2k$ such z_{i+1}, we have that $|B'|$ is trivially bounded above by $4k$. Hence the path $z_0 \to \cdots \to z_m$ is contained in a subgraph H of G_n in which we restrict vertices to only have letters from B'. The result follows immediately as $H \cong G_{4k}$. □

From Lemma 4.7 we may define, for a given rule set Π_k, the *eventual diameter* of the word graph family $\mathrm{WGF}(\Pi_k)$ as $\mathrm{Diam}(\mathrm{WG}(\Pi_k, 4k)$, and note from Lemma 4.5 and Lemma 4.6 that the eventual diameter of $\mathrm{WGF}(\Pi_k)$ is between k and $2k$. Further we note that we may lower $4k$ to $3k$ in Lemma 4.7 but for the sake of simplicity we omit doing so.

We now give a result which allows us to significantly restrict which potential rule sets Π_k we may consider of interest with regard to the degree-diameter problem.

Proposition 4.8. *A word graph family* $\mathrm{WGF}(\Pi_k)$ *is asymptotically close to the Moore bound if, and only if, its eventual diameter is k.*

Proof. Let $\mathrm{WGF}(\Pi_k) = \{\mathrm{WG}(\Pi_k, k+1), \mathrm{WG}(\Pi_k, k+2), \dots\}$ and denote $\mathrm{WG}(\Pi_k, n)$ by G_n as previously. Let $G_n \in \mathrm{WGF}(\Pi_k)$ for some $n \geq 4k$. Define ε such that the eventual diameter of $\mathrm{WGF}(\Pi_k)$ is $k + \varepsilon$. From Lemma 4.4 the degree of G_n is $n - k + |\Pi_k|$, hence taking $\alpha = |\Pi_k| - k$ we have $\mathrm{Deg}(G_n) = \alpha + n$. We count the size of G_n as follows

$$|\,\mathrm{V}(G_n)| = k!\binom{n}{k} = n(n-1)\dots(n-(k-1)) = n^k + \mathcal{O}(n^{k-1}).$$

We recall that the Moore bound for a directed graph is given by $\mathrm{DM}(d,k) = d^k + d^{k-1} + \cdots + 1 = d^k + \mathcal{O}(d^{k-1})$. Letting $d_n = \mathrm{Deg}(G_n)$ and $k_n = \mathrm{Diam}(G_n)$, we have

$$\begin{aligned}
\lim_{n\to\infty}\left\{\frac{|\,\mathrm{V}(G_n)|}{\mathrm{DM}(d_n,k_n)}\right\} &= \lim_{n\to\infty}\left\{\frac{n^k + \mathcal{O}(n^{k-1})}{\mathrm{DM}(n+\alpha, k+\varepsilon)}\right\} \\
&= \lim_{n\to\infty}\left\{\frac{n^k + \mathcal{O}(n^{k-1})}{(n+\alpha)^{k+\varepsilon} + \mathcal{O}(n^{k+\varepsilon-1})}\right\} \\
&= \lim_{n\to\infty}\left\{\frac{n^k + \mathcal{O}(n^{k-1})}{n^{k+\varepsilon} + \mathcal{O}(n^{k+\varepsilon-1})}\right\}
\end{aligned}$$

$$= \begin{cases} 1, & \text{if } \varepsilon = 0, \\ 0, & \text{otherwise.} \end{cases}$$ □

We see that any choice of Π_k for which we get an eventual diameter other than k can only be interesting in the degree-diameter problem for small graphs. As we are concerned with finding families of graphs with best asymptotic behaviour, we therefore ignore choices of Π_k which result in an eventual diameter more than k. Therefore we shall call a rule set Π_k *admissible* if the eventual diameter of $\mathrm{WGF}(\Pi_k)$ is k, and from now on will only consider admissible choices of Π_k.

4.6 Shift-Restricted Word Graphs

We now introduce a further restriction to the potential rule sets Π_k that we shall consider. Though the restriction is significant, it is both a natural restriction and is met by both the Gómez graphs and the Faber-Moore-Chen graphs.

We shall call a rule set Π_k *shift restricted* if for any $\pi \in \Pi_k$ we have $\pi(i) \leq i + 1$. Recalling that the alphabet fixing adjacencies of a word graph are defined by $x_1x_2 \dots x_k \to x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(k)}$, we may informally think of being shift restricted meaning that no letter in the word $x_1x_2 \dots x_k$ may be moved more than one space to the left by any alphabet fixing rule. We now derive further basic properties satisfied by shift restricted word graphs.

Let Π_k be an admissible and shift restricted rule set and let $G_n = \mathrm{WG}(\Pi_k, n) \in \mathrm{WGF}(\Pi_k)$ defined over an alphabet B for some $n > k$. For all $v \in \mathrm{V}(G_n)$ and $x \in B$ we now define the function $p_x(v)$ which is the *position* of the letter x in the word v. We define $p_x(v)$ by $p_{x_i}(x_1x_2 \dots x_k) = i$ and $p_y(x_1x_2 \dots x_k) = 0$ if $y \notin \{x_1, x_2, \dots, x_k\}$.

Lemma 4.9. *For any $u, v \in \mathrm{V}(G_n)$ such that $u \to v$ and any $y \in B$ we have $p_y(v) \geq p_y(u) - 1$.*

Proof. If $p_y(u) = 0$ then the result is immediate as $p_y(v') \geq 0$ for all $v' \in \mathrm{V}(G_n)$. Hence, suppose that $u = x_1x_2 \dots x_k$ and $y = x_i$ for some $1 \leq i \leq k$. If $u \to v$ by an alphabet changing rule then $v = x_2x_3 \dots x_kz$ for some $z \notin \{x_1, x_2, \dots, x_k\}$ and $p_y(v) = p_{x_i}(x_2x_3 \dots x_kz) = i - 1 = p_y(u) - 1$. Otherwise, we have $u \to v$ by an alphabet fixing rule, in which case $v = x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(k)}$ for some $\pi \in \Pi_k$. Letting $\pi(j) = i$ we have $p_{x_i}(v) = p_{x_j}(u) = j \geq \pi(j) - 1 = i - 1 = p_{x_i}(u) - 1$. □

This lemma formalises the implication of shift restriction on movement of letters between rule applications, and has the following immediate and useful corollary.

Corollary 4.10. *For any $u, v \in \mathrm{V}(G_n)$ and $y \in B$, all paths connecting u to v must have length at least $p_y(u) - p_y(v)$. (In the case that $p_y(u) = 0$ and $p_y(v) > 0$ we can change this to a minimum length of $k + 1 - p_y(v)$).*

Proof. This follows from a trivial induction using Lemma 4.9. □

Lemma 4.11. *For Π_k is shift restricted and $G_n = \mathrm{WG}(\Pi_k, n)$, we have $\mathrm{Diam}(G_n) \geq k$.*

Proof. Taking $u, v \in \mathrm{V}(G_n)$ to be $u = x_1 x_2 \dots x_k$ and $v = x_1 x_2 \dots x_{k-1} y$ for some $y \notin \{x_1, x_2, \dots, x_k\}$ we have $p_{x_k}(u) = k$ and $p_{x_k}(v) = 0$, hence from Corollary 4.10 we have that any path connecting u and v is at least length k. □

Lemma 4.12. *For Π_k is shift restricted and $G_n = \mathrm{WG}(\Pi_k, n)$, we have $\mathrm{Diam}(G_n) \leq k$.*

Proof. As Π_k is admissible by assumption, we have that the eventual diameter of $\mathrm{WGF}(\Pi_k)$ is k, and so $\mathrm{Diam}(G_n) = k$ for all $n \geq 4k$. Hence, consider some $u, v \in \mathrm{V}(G_n)$ for some $n < 4k$. Let $\phi : G_n \to G_{4k}$ be the inclusion from G_n to G_{4k} and consider a shortest path from $u' = \phi(u)$ to $v' = \phi(v)$ in G_{4k}. Letting $B' = \alpha(u') \cup \alpha(v')$ we can see that for any vertex $w' \in \mathrm{V}(G_{4k})$ satisfying $\alpha(w') \subseteq B'$ there exists a vertex $w \in \mathrm{V}(G_n)$ such that $\phi(w) = w'$. Suppose that on a path from u' to v' we introduce a letter $y \notin B'$ via an alphabet changing rule, call the vertex after this rule w'. We have $p_y(w') = k$ and $p_y(v') = 0$, so by Lemma 4.10 any path connecting w' and v' is at least length k, and thus a path connecting u' and v' containing w' is at least length $k + 1$. However, we have $\mathrm{Diam}(G_{4k}) = k$ so a shortest path from u' to v' is length at most k, so no such vertex w' exists. Therefore any vertex w' on the shortest path from u' to v' satisfies $\alpha(w') \subseteq B'$, and so there exists a vertex $w \in \mathrm{V}(G_n)$ such that $\phi(w) = w'$, and the shortest path from u' to v' in G_{4k} corresponds to a shortest path from u to v in G_n, which immediately gives $\mathrm{Diam}(G_n) \leq k$. □

Combining our results we have shown that, for all n, $\mathrm{Diam}(G_n) = k$. We can now state the following important corollary of our work.

Corollary 4.13. *If Π_k and T_k are admissible shift restricted rule sets, and $|\Pi_k| < |\mathrm{T}_k|$, then every $G_n \in \mathrm{WGF}(\Pi_k)$ and $H_n \in \mathrm{WGF}(\mathrm{T}_k)$ satisfy $\mathrm{Diam}(G_n) = \mathrm{Diam}(H_n)$ and $|\mathrm{V}(G_n)| = |\mathrm{V}(H_n)|$ for all n, but we have $\mathrm{Deg}(G_n) < \mathrm{Deg}(H_n)$ for all n.*

We now make the definition that an admissible and shift restricted rule set Π_k is *optimal* if there does not exist another admissible and shift restricted rule set T_k such that $|\,\mathrm{T}_k\,| < |\Pi_k|$.

With our now established definition of optimality, we now aim to show that the rule sets of the Gómez graphs are optimal.

4.7 Optimality of Gómez Graphs

In this section, suppose that Π_k is an admissible shift restricted rule set.

Lemma 4.14. *For each $1 \leq i \leq n$ there exists some $\pi \in \Pi_n$ which contains an i-cycle.*

Remark. The formal proof of this lemma obscures the fact this is essentially a simple observation. We first illustrate the idea behind the proof. Consider for $k = 9$ a path of length k from the vertex $u = x_1x_2x_3x_4x_5x_6x_7x_8x_9$ to the vertex $v = y_1y_2y_3y_4x_9x_1x_2x_3x_4$ where $y_1, y_2, y_3, y_4 \notin \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}$. Let $z_0 = u \to z_1 \to \cdots \to z_k = v$ be a path from u to v. We illustrate an example path from u to v, and note that the key idea is that at some point in that path x_k has to "jump" the block of $y_1y_2y_3y_4$ via an alphabet fixing rule, and that jump corresponds to a 5-cycle in the alphabet fixing rule.

z_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
z_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	y_1
z_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	y_1	y_2
z_3	x_4	x_5	x_6	x_7	x_8	x_9	y_1	y_2	y_3
z_4	x_5	x_6	x_7	x_8	x_9	y_1	y_2	y_3	y_4
z_5	x_6	x_7	x_8	x_5	y_1	y_2	y_3	y_4	x_9
z_6	x_7	x_8	x_5	y_1	y_2	y_3	y_4	x_9	x_1
z_7	x_8	x_5	y_1	y_2	y_3	y_4	x_9	x_1	x_2
z_8	x_5	y_1	y_2	y_3	y_4	x_9	x_1	x_2	x_3
z_9	y_1	y_2	y_3	y_4	x_9	x_1	x_2	x_3	x_4

The example path given is from the Gómez graph $\mathrm{GG}(9, 9)$, and the 5-cycle occurs in the alphabet fixing rule between z_4 and z_5.

Proof. For each $j \geq 1$ we shall show the existence of a $(j+1)$-cycle, noting that when $j + 1 = k - 1$ we will have shown the existence of a permutation made of a $k - 1$ cycle and, therefore, also a 1-cycle. Let $u = x_1x_2 \ldots x_k$ and $v = y_1y_2 \ldots y_jx_kx_1x_2 \ldots x_{k-j}$. As $p_{y_1}(u) = 0$ and $p_{y_1}(v) = 1$ we must have that a shortest path connecting u and v is length k. Hence, let $z_0 = u \to z_1 \to \cdots \to z_k = v$ be a shortest path connecting u and

v. A trivial induction with Lemma 4.9 shows that $p_{y_1}(z_i) = k - i + 1$ for $i \geq 1$, and similarly that $p_{y_j}(z_i) = k - i + j$ for $i \geq i$.

Now we consider the position of x_k in each z_i. First we start from z_k and move backwards in the path. At z_k we have $p_{x_k}(z_k) = j + 1$. At each z_{k-i} we have $p_{x_k}(z_{k-i}) \leq j + 1 + i$. Now we start from z_0 and move forwards. We have $p_{x_k}(z_0) = k$, and at each i we have $p_{x_k}(z_i) \geq k - i$. Combining these we have $k - i \leq p_{x_k}(z_i) \leq k - i + j + 1$. As $p_{y_j}(z_i) = k - i + j$ we must have at each z_i that either $p_{x_k}(z_i) = k - i$ or $p_{x_k}(z_i) = k - i + j + 1$.

Finally, as $p_{x_k}(z_0) = k$ and $p_{x_k}(z_k) = j + 1$ there must be some point in the path, say α, such that $p_{x_k}(z_\alpha) = k - \alpha$ and $p_{x_k}(z_{\alpha+1}) = k - \alpha + j$. As this cannot happen in an alphabet changing rule, the vertices z_α and $z_{\alpha+1}$ must be connected by an alphabet fixing rule $\pi \in \Pi_k$. Finally, the rule π must contain the $(j + 1)$-cycle $((k - (\alpha + 1))\ (k - (\alpha + 2))\ \ldots\ (k - (\alpha + j + 1)))$. □

This now allows us to give our optimality result concerning the Gómez graphs.

Proposition 4.15. *The rule sets Π_k of the Gómez graphs are optimal.*

Proof. We shall consider the cases of odd k and even k separately.

If $k = 2n + 1$ is odd, then the rule sets Π_k of the Gómez graphs are given as follows

$$\begin{aligned}\Pi_k = \{&(1\ 2\ \ldots\ k),\\ &(2\ 3\ \ldots\ k),\\ &(1\ 2)(3\ 4\ \ldots\ k),\\ &\ldots\\ &(1\ 2\ \ldots\ n)((n+1)\ (n+2)\ \ldots\ k)\}.\end{aligned} \tag{4.3}$$

From this definition we immediately see that every cycle of length 1 to k occurs exactly once in a permutation in Π_k and as a result the set Π_k is as small as possible with the property of Lemma 4.14.

If $k = 2n$ is even, then the rule sets Π_k of the Gómez graphs are also given by equation 4.3 with our new definition of n. In this case we see that each cycle of length 1 to k except n occurs exactly once in a permutation in Π_k, and that there are two cycles of length n in permutations in Π_k. It is clear that there is no way to eliminate a permutation from the set Π_k by removing one cycle of length k, and so the set Π_k is also as small as possible with the property of Lemma 4.14. □

Altogether we have shown that the Gómez graphs are optimal, and thus provide the largest possible graphs for given degree and diameter amongst word graphs formed from admissible and shift restricted rule sets. If we wish to modify the definition of the Gómez graphs or Faber-Moore-Chen graphs further to attempt to create better graphs for given degree and diameter then we will need to either break the property of admissibility and consider small graphs or break the property of shift restrictedness.

4.8 When Word Graphs are Cayley

From the definition of word graphs we have the following trivial observation.

Proposition 4.16. *For any rule set Π_k and $n > k$ the word graph $G_n = \mathrm{WG}(\Pi_k, n)$ is vertex-transitive.*

Proof. Let B be the alphabet G_n is defined over. Let $x = x_1x_2 \dots x_k$ and $y = y_1y_2 \dots y_k$ be arbitrary vertices in $\mathrm{V}(G_n)$. Let $\pi \in S_n$ be a permutation acting on B such that $\pi(x_i) = y_i$ for all $1 \leq i \leq k$, and the action of π on other members of B is arbitrary. The action of π on $\mathrm{V}(G_n)$ given by $\pi(u) = \pi(u_1u_2 \dots u_k) = \pi(u_1)\pi(u_2) \dots \pi(u_k)$ is an automorphism of G_n, and further $\pi(x) = y$. This is clear as π is a relabelling of the letters of the vertices, and the definition of the adjacencies of any vertex $u \in \mathrm{V}(G_n)$ is independent of the labelling of its letters. □

In fact, from this proof we have the following useful observation.

Proposition 4.17. *For a word graph $G_n = \mathrm{WG}(\Pi_k, n)$ there is a subgroup H of the automorphism group $\mathrm{Aut}(G_n)$ of G_n which is isomorphic to S_n and acts regularly on the vertices of G_n.*

Proof. Simply take the extension of the natural action of S_n on the alphabet B of $\mathrm{V}(G_n)$ as described in the previous proof as the group H. □

This immediately shows us that word graphs give us examples of not just digraphs but vertex-transitive digraphs. Given this fact, a more difficult question to then answer is determining when word graphs are also Cayley. For the Faber-Moore-Chen digraphs, this question was answered in [50]. The method used in this paper is to determine the automorphism group of the Faber-Moore-Chen digraphs and then use a classification of parameters (n, k) for which there is a subgroup of the symmetric group S_n which acts regularly on k-tuples. This result can be found in [20, 10, 53].

We summarise the result here in a table. In the following table the groups M_{11} and M_{12} are the Mathieu groups.

k	n	Group
m	m	S_m
m	$m+1$	S_{m+1}
m	$m+2$	A_{m+2}
2	q	Affine transformations over finite near-fields
3	$q+1$	$\mathrm{PGL}(2,q), G(2,q)$
4	11	M_{11}
5	12	M_{12}

For the affine transformations over finite near-fields, letting F be a finite near field (i.e. an algebraic structure satisfying the field axioms with the possible exceptions of the multiplicative commutative law and the left distributive law), we have that sharply 2-transitive groups are in one-to-one correspondence with groups of affine transformations of the form $x \prod ax + b$ for $a, b \in F$ and $a \neq 0$.

The group which we denote by $G(2,q)$ exists for each q which is an odd square. In this case, the outer automorphism of $\mathrm{PSL}(2,q)$ is a Klein group $\{1, a, b, c\}$ where $\mathrm{PSL}(2,q)\{1,a\} = \mathrm{PGL}(2,q)$, and b is induced by the field automorphism of order 2. In this case, we define $G(2,q) = \mathrm{PSL}(2,q)\{1,c\}$, which is also sharply 3-transitive.

This gives the following immediate corollary.

Corollary 4.18. *For any k, n from the above table, the word graph $\mathrm{WG}(\Pi_k, n)$ is Cayley.*

Proof. We use the characterisation of Cayley graphs from Proposition 1.1. □

We also make the following trivial extension of this corollary, as we shall find for the word graphs we consider that $\mathrm{Aut}(\mathrm{WG}(\Pi_k, n)) \cong S_n$.

Corollary 4.19. *If $\mathrm{Aut}(\mathrm{WG}(\Pi_k, n)) \cong S_n$ then the graph $\mathrm{WG}(\Pi_k, n)$ is Cayley if, and only if, k and n are in the above table.*

Hence we now create a test to help determine if the automorphism group of a given word graph is isomorphic to the symmetric group. Note that the test we develop will only provide a sufficient condition, but not a necessary one.

4.8.1 Automorphism Group Test

To create our test, we first need some definitions. We begin by letting Γ_k denote the Cayley graph $\mathrm{Cay}(\Pi_k, S_k)$ and again use G_n to denote $\mathrm{WG}(\Pi_k, n)$.

Lemma 4.20. *If H is a subgraph of G_n induced by vertices $v \in \mathrm{V}(G_n)$ with $\alpha(v) = \{x_1, x_2, \dots x_k\} \subset B$ then we have $H \cong \Gamma_k$.*

Proof. If we choose a vertex $x_1x_2 \dots x_k$ in H to identify with the vertex e in Γ_k, then for each $\pi \in S_k$ the identification of $x_{\pi(1)}x_{\pi(2)} \dots x_{\pi(k)}$ in H with π in Γ_k is an isomorphism. □

We shall now refer to Γ_k as the *alphabet fixing subgraph* of G_n. We shall also refer to any subgraph of G_n induced by all vertices sharing an alphabet as the alphabet fixing subgraph, noting that they are isomorphic to Γ_k and thus unique to isomorphism.

We make two further definitions now. First, we shall call a word graph G_n *alphabet stable* if there exists no automorphism $\phi \in \mathrm{Aut}(G_n)$ such that there exist some $u, v \in \mathrm{V}(G_n)$ with $\alpha(u) = \alpha(v)$ but $\alpha(\phi(u)) \neq \alpha(\phi(v))$. In other words, a word graph is alphabet stable if, and only if, it preserves whether arcs are alphabet fixing or alphabet changing. Second, we shall call a family of word graphs $\mathrm{WGF}(\Pi_k)$ *subregular* if the alphabet fixing subgraph Γ_k of G_n is regular (i.e. $\mathrm{Aut}(\Gamma_n) \cong S_n$).

In the following let G_n be a word graph which is both alphabet stable and subregular. We aim to show that $\mathrm{Aut}(G_n) \cong S_n$.

Lemma 4.21. *If $\phi \in \mathrm{Aut}(G_n)$ fixes a vertex u then ϕ fixes all v such that $\alpha(u) = \alpha(v)$.*

Proof. Letting $V = \{v \in \mathrm{V}(G_n) | \alpha(v) = \alpha(u)\}$, consider $\psi = \phi|_V$, the restriction of ϕ to the alphabet fixing subgraph of G_n induced by V. For all $v \in V$ we have $\alpha(\psi(v)) = \alpha(\phi(v)) = \alpha(\phi(u)) = \alpha(u)$ due to alphabet stability, which shows $\psi(v) \in V$. Therefore, as ϕ is an automorphism, we have that ψ is injective from V to V and thus bijective. Hence ψ is an automorphism of the vertices of G_n in V to themselves, i.e. ψ is an automorphism of the alphabet fixing subgraph of G_n. As G_n is subregular, any automorphism of Γ_k fixing a single vertex is the identity. Therefore, as $\psi(u) = u$ we must have that ψ is the identity on V. □

Next we introduce a technical lemma which will be required in an induction.

Lemma 4.22. *If $\phi \in \mathrm{Aut}(G_n)$ and $X, Y, Z \subset B$ with the following properties*

i) $X = \{x_1, x_2, z_1, z_2, \dots, z_{k-2}\}$,

ii) $Y = \{y_1, y_2, z_1, z_2, \dots, z_{k-2}\}$,

iii) $Z = \{x_2, y_2, z_1, z_2, \ldots, z_{k-2}\}$,

iv) ϕ *fixes all* $v \in \mathrm{V}(G_n)$ *such that* $\alpha(v) = X$ *or* $\alpha(v) = Y$,

then ϕ *fixes all* $v \in \mathrm{V}(G_n)$ *such that* $\alpha(v) = Z$.

Proof. Let $u = x_1z_1z_2 \ldots z_{k-2}x_2$ and $v = y_1z_1z_2 \ldots z_{k-2}y_2$ and let $w, w' \in \mathrm{V}(G_n)$ such that $u \to w, v \to w'$ and $\alpha(w) = \alpha(w')$. As $|X \cap Y| = k - 2$, we must have that both $u \to w$ and $v \to w'$ are alphabet changing rules. Therefore, we must have $x_1 \notin \alpha(w), x_2 \in \alpha(w), y_1 \notin \alpha(w')$ and $y_2 \in \alpha(w')$. Hence we have $\alpha(w) \supseteq (X \cap Y) \cup \{x_2, y_2\} = Z$. We also have $|\alpha(w)| = k = |Z|$, so $\alpha(w) = Z$. We now see that $u \to w$ must be the alphabet changing rule which introduces y_2, and so $w = x_2z_1z_2 \ldots z_{k-2}y_2$ and similarly $w' = y_2z_1z_2 \ldots z_{k-2}x_2$. From our assumptions we have $\phi(u) = u, \phi(v) = v$ and $\alpha(\phi(w)) = \alpha(\phi(w'))$ as $\alpha(w) = \alpha(w')$ and G_n is alphabet stable. As a result we see $u \to \phi(w)$ and $v \to \phi(w')$ with $\alpha(\phi(w)) = \alpha(\phi(w'))$, so we have $\phi(w) = w$ and $\phi(w') = w'$. Now applying Lemma 4.21 we have the desired result. □

Lemma 4.23. *The only automorphism* $\phi \in \mathrm{Aut}(G_n)$ *which fixes a vertex* $u \in \mathrm{V}(G_n)$ *and all* $v \in \mathrm{V}(G_n)$ *such that* $u \to v$ *is the identity.*

Proof. Label u as $x_1x_2 \ldots x_k$ and the alphabet B of G_n as $\{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_{n-k}\}$. For a vertex $v \in \mathrm{V}(G_n)$ we define the function $f(v) = |\{x_1, x_2, \ldots x_k\} \cap \alpha(v)|$. We shall show by induction for $k \geq i \geq 0$ that ϕ fixes all v such that $f(v) = i$.

For $i = k$, for any $v \in \mathrm{V}(G_n)$ with $f(v) = k$ we have $\alpha(v) = \alpha(u)$ and u is fixed by ϕ. Hence, by Lemma 4.21 we have that ϕ fixes v also.

For $i = k - 1$, let $v \in \mathrm{V}(G_n)$ be a vertex with $f(v) = k - 1$. We first consider $\alpha(v) = \{x_2, x_3, \ldots, x_k, y\}$. In this case, the vertex $v' = x_2x_3 \ldots x_ky$ satisfies $u \to v'$ and so v' is fixed by ϕ. Again, using Lemma 4.21 and $\alpha(v) = \alpha(v')$ we show that ϕ fixes v. For other v with $f(v) = k - 1$, letting $y \in \alpha(v)$, we have $|\alpha(v) \cap \{x_1, x_2, \ldots, x_k\}| = k - 1$ and $|\alpha(v) \cap \{x_2, x_3, \ldots, x_k, y\}| = k - 1$. Applying Lemma 4.22 to the sets $X = \{x_1, x_2, \ldots, x_k\}, Y = \{x_2, x_3, \ldots, x_k, y\}$ and $Z = \alpha(v)$ we see that v is fixed.

For $i = c$, given the inductive hypothesis for $i = c + 1$, without loss of generality let $v \in \mathrm{V}(G_n)$ such that $\alpha(v) = \{x_1, x_2, \ldots, x_c, y_1, y_2, \ldots, y_{k-c}\}$. We now apply Lemma 4.22 to the sets $X = \{x_1, x_2, \ldots, x_{c+1}, y_1, y_2, \ldots, y_{k-c-1}\}$,

$Y = \{x_1, x_2, \ldots, x_{c+1}, y_2, y_3, \ldots, y_{k-c}\}$ and $Z = \{x_1, x_2, \ldots, x_c, y_1, y_2, \ldots, y_{k-c}\}$ to get the desired result. □

We are now in a position to prove our main result on the implication of alphabet stability and subregularity of a word graph.

Proposition 4.24. *If a word graph* $G_n = \mathrm{WG}(\Pi_k, n)$ *is alphabet stable and subregular then* $\mathrm{Aut}(G_n) \cong S_n$.

Proof. Let $H \subseteq \mathrm{Aut}(G_n)$ as defined in Proposition 4.21. Suppose that $\phi \in \mathrm{Aut}(G_n)$. Consider $u \in \mathrm{V}(G_n)$ and define $\psi \in H$ such that $\psi(\phi(u)) = u$ and for all $v \in \mathrm{V}(G_n)$ such that $u \to v$ via an alphabet changing rule we have $\psi(\phi(v)) = v$. Note that ψ is guaranteed to exist as, if we label $u = x_1x_2 \ldots x_k$ then the requirement $\psi(\phi(u)) = u$ corresponds to choosing an action of ψ on the set $\{x_1, x_2, \ldots, x_k\}$, and if we label each $v = x_2x_3 \ldots x_ky_i$ where $B = \{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_{n-k}\}$ then the requirements $\psi(\phi(v)) = v$ determine the action of ψ on each of the remaining y_i. Finally, we have that $\phi \circ \psi$ fixes u and all v such that $u \to v$, so by Lemma 4.23 we must have $\phi \circ \psi$ is the identity, and therefore $\psi = \phi^{-1}$ and $\phi \in H$. □

Altogether we have established that alphabet stability and subregularity are sufficient conditions to show that $\mathrm{Aut}(G_n) \cong S_n$. We now devote the rest of this section to creating tests to determine alphabet stability and subregularity. Our tests shall only concern counting certain paths in the alphabet fixing subgraph of a word graph, which will allows us to determine whether $\mathrm{Aut}(\mathrm{WG}(\Pi_k, n)) \cong S_n$ for all word graphs in a family $\mathrm{WGF}(\Pi_k)$ by a finitely computable test on the graph $\mathrm{Cay}(\Pi_k, S_k)$.

Lemma 4.25. *If* $u, v \in \mathrm{V}(G_n)$ *such that* $u \to v$ *by an alphabet changing rule, then there is a unique shortest path of length* k *from* v *to* u.

Proof. We label $u = x_1x_2 \ldots x_k$ and $v = x_2x_3 \ldots x_ky$. First, by considering $p_{x_1}(v) = 0$ and $p_{x_1}(u) = 1$ and using Lemma 4.9 we see that a path connecting v to u must be length at least k, and as $\mathrm{Diam}(G_n) = k$ we therefore know a shortest path connecting v to u is length k. Now consider a path $z_0 = v \to z_1 \to \cdots \to z_k = u$, by considering Corollary 4.10 and $p_{x_i}(z_i)$ we see that each $z_{i-1} \to z_i$ must be connected by the alphabet changing rule introducing x_i. Hence the path $z_0 \to z_1 \to \cdots \to z_k$ is a uniquely defined path of length k joining v to u. □

Now suppose that for all $u, v \in \mathrm{V}(\Gamma_k)$ with $u \to v$ there is either more than one path of length k connecting v to u, or there is at least one path of length less than k connecting v to u.

Lemma 4.26. *There is no $\phi \in \mathrm{Aut}(G_n)$ such that $\alpha(\phi(v)) \neq \alpha(u)$.*

Proof. Suppose that such a ϕ exists. As $u \to v$ we have $\phi(u) \to \phi(v)$, and as $\alpha(\phi(u)) \neq \alpha(\phi(v))$ we have that $\phi(u) \to \phi(v)$ by an alphabet changing rule. By Lemma 4.25 there is a unique shortest path of length k connecting $\phi(v)$ to $\phi(u)$. However, by assumption we have that there is either a path of length less than k connecting v to u or multiple paths of length k connecting v to u. Therefore no such ϕ can exist. □

Lemma 4.27. *Under the above assumptions, G_n is alphabet stable.*

Proof. Suppose that G_n is not alphabet stable. Let $\phi \in \mathrm{Aut}(G_n)$ and $u, v \in \mathrm{V}(G_n)$ such that $\alpha(u) = \alpha(v)$ and $\alpha(\phi(u)) \neq \alpha(\phi(v))$. Now let $z_0 = u \to z_1 \to \cdots \to z_m = v$, $m \leq k$ be a shortest path connecting u and v. Suppose some z_i has $\alpha(z_i) \neq \alpha(u)$. Let i be as small as possible with this property, and let $u = x_1 x_2 \dots x_k$. We then have $z_i = x_{\pi(1)} x_{\pi(2)} \dots x_{\pi(k-1)} y$ and $z_m = v = x_{\tau(1)} x_{\tau(2)} \dots x_{\tau(k)}$ for some permutations $\pi, \tau \in S_k$. As $p_y(z_i) = k$ and $p_y(z_m) = 0$ we have from Corollary 4.10 that a path connecting z_i and z_m is at least length k, but this implies that the path $z_0 \to z_1 \to \cdots \to z_m$ is at least length $k + i$, contradicting that it is a shortest path. As a result we see there is no such z_i and we have $\alpha(z_i) = \alpha(u)$ for all $0 \leq i \leq m$. Now, as $\alpha(\phi(z_0)) \neq \alpha(\phi(z_m))$ there is a smallest i such that $\alpha(\phi(z_i)) \neq \alpha(\phi(z_{i+1}))$. So z_i and z_{i+1} satisfy $\alpha(z_i) = \alpha(z_{i+1})$ but $\alpha(\phi(z_i)) \neq \alpha(\phi(z_{i+1}))$, contradicting Lemma 4.26. Hence, G_n must be alphabet stable. □

Lemma 4.28. *If Γ_k is not regular, then there exists an automorphism $\phi \in \mathrm{Aut}(\Gamma_k)$ such that for some $u, v \in \mathrm{V}(\Gamma_k)$ with $u \to v$ we have $\phi(u) = u$ but $\phi(v) \neq v$.*

Proof. Let $H < \mathrm{Aut}(\Gamma_k)$ be regular and let $\phi \in \mathrm{Aut}(\Gamma_k) \setminus H$. Consider $u \in \mathrm{V}(\Gamma_k)$ and let $\psi \in H$ be the automorphism such that $\psi(\phi(u)) = u$. Let $\phi' = \psi \circ \phi$, so ϕ' fixes u. As $\phi' \notin H$ we must have ϕ' is not the identity. Threfore, there exists some $v \in \mathrm{V}(\Gamma_k)$ such that $\phi'(v) \neq v$. Consider a path $z_0 = u \to z_1 \to \cdots \to z_m = v$ from u to v. On this path there must exists some i such that $z_i = \phi'(z_i)$ but $z_{i+1} \neq \phi'(z_{i+1})$. □

Corollary 4.29. *If for all $u, v, w \in \mathrm{V}(\Gamma_k)$ with $u \to v$ and $u \to w$ these exists some i such that the number of paths of length i from v to u and the number of paths of length i from w to u are different, then Γ_k is regular, and $\mathrm{WGF}(\Pi_k)$ is subregular.*

We now combine these results and state our test. Let $G_n = \mathrm{WG}(\Pi_k, n) \in \mathrm{WGF}(\Pi_k)$ with alphabet fixing subgraph $\Gamma_k = \mathrm{Cay}(\Pi_k, S_k)$. Let $u \in \mathrm{V}(\Gamma_k)$ and let $\{v_i\}$ be the set of vertices such that $u \to v_i$.

Proposition 4.30. *If the following conditions hold, then* $\mathrm{Aut}(G_n) \cong S_n$.

i) for each v_i, v_j *there exists some* m *such that the number of paths from* v_i *to* u *of length* m *is different to the number of paths from* v_j *to* u *of length* m*;*

ii) each v_i *has either a path of length less than* k *to* u *or has more than one path of length* k *to* u*.*

We now demonstrate the use of this proposition by applying it to small cases for the Faber-Moore-Chen graphs and Gómez graphs via direct computation.

4.8.2 Computational Results

First we apply Proposition 4.30 to the Faber-Moore-Chen graphs.

Let $\pi_i = (1\ 2\ \ldots\ i)$ and let $\Pi_k = \{\pi_2, \pi_3, \ldots, \pi_k\}$. The Faber-Moore-Chen graphs are given by $\mathrm{WG}(\Pi_k, n)$ for all k and all $n > k$. Considering the alphabet fixing subgraph Γ_k of the Faber-Moore-Chen graphs, we now count paths of each length $1 \leq i \leq k-1$ from each π_j to e in Γ_k. We summarise our results in tables.

For $k = 3$

	π_2	π_3
1	1	0
2	-	1

For $k = 4$

	π_2	π_3	π_4
1	1	0	0
2	-	1	0
3	-	-	1

For $k = 5$

	π_2	π_3	π_4	π_5
1	1	0	0	0
2	-	1	0	0
3	-	-	1	0
4	-	-	-	1

In these examples, we see that from each π_{i+1} there is exactly one shortest path of length i to e. Hence for each of these examples we meet condition (ii) of Proposition 4.30 as each π_{i+1} has a path of length less than k to e, and we meet

condition (i) as, for $i < j$, there is a path of length i from π_{i+1} to e, but no path of length i from π_{j+1} to e. Later we shall prove this property for all k to demonstrate our method in the much simpler case of the Faber-Moore-Chen graphs.

For the Gómez graphs let
$\pi_i = (1\ 2\ \ldots\ (\lfloor k/2 \rfloor - i))((\lfloor k/2 \rfloor - i + 1)\ (\lfloor k/2 \rfloor - i + 2)\ \ldots\ k)$. So for $k = 5$ we have $\pi_0 = (1\ 2)(3\ 4\ 5)$, $\pi_1 = (2\ 3\ 4\ 5)$ and $\pi_2 = (1\ 2\ 3\ 4\ 5)$. Let $\Pi_k = \{\pi_0, \pi_1, \ldots, \pi_{\lfloor k/2 \rfloor}\}$. The Gómez graphs are given by $\mathrm{WG}(\Pi_k, n)$ for all k and $n > k$. Considering the alphabet fixing subgraph Γ_k of the Gómez graphs, we now count paths of length $i = k-1, k$ from each π_j to e in Γ_k.

For $k = 5$

	π_0	π_1	π_2
4	-	-	1
5	4	2	1

For $k = 7$

	π_0	π_1	π_2	π_3
6	-	-	-	1
7	7	4	2	1

For $k = 9$

	π_0	π_1	π_2	π_3	π_4
8	-	-	-	-	1
9	11	7	4	2	1

For $k = 4$

	π_0	π_1	π_2
3	2	-	2
4	3	5	2

For $k = 6$

	π_0	π_1	π_2	π_3
5	4	-	-	4
6	8	13	5	2

For $k = 8$

	π_0	π_1	π_2	π_3	π_4
7	8	-	-	-	8
8	19	33	13	5	2

4.8.3 Example: Faber-Moore-Chen

We now aim to apply the test of Proposition 4.30 to the Faber-Moore-Chen graphs to re-derive the result of [50] and illustrate our method.

Let $\pi_i = (1\ 2\ \ldots\ i)$, $\Pi_k = \{\pi_2, \pi_3, \ldots, \pi_k\}$ and $\Gamma_k = \mathrm{Cay}(\Pi_k, S_k)$ be the alphabet fixing subgraph of the Faber-Moore-Chen graphs $G_n = \mathrm{WG}(\Pi_k, n)$ as before.

Lemma 4.31. *For $2 \leq i \leq k$ the shortest path from π_i to e in Γ_k is length $i-1$.*

Proof. We use the notation of Γ_k as a subgraph of G_n. In this notation, the vertex π_i is equivalent to $u = x_2x_3 \ldots x_ix_1x_{i+1}x_{i+2} \ldots x_k$, and the vertex e is equivalent to $v = x_1x_2 \ldots x_k$. From Corollary 4.10 and the fact $p_{x_1}(u) = i$ and $p_{x_1}(v) = 1$ we have that a minimum path connecting u and v must be at least length $i-1$. Further, as π_i is an i-cycle we have $\pi^i = e$ and hence the adjacencies corresponding to the rules π_i form a path of length $i-1$ to e. □

From this we have all that we need to apply the test of Proposition 4.30.

Proposition 4.32. *The Faber-Moore-Chen graphs $G_n = \mathrm{WG}(\Pi_k, n)$ have $\mathrm{Aut}(G_n) \cong S_n$.*

Proof. We apply Proposition 4.30. Letting $\Gamma_k = \mathrm{Cay}(\Pi_k, S_k)$, for vertices $\pi_i, \pi_j \in \mathrm{V}(\Gamma_k)$ with $i < j$ we have that there is a shortest path from π_i to e of length $i-1$ but that there is no path of length $i-1$ from π_j to e. Therefore condition (i) of Proposition 4.30 is satisfied. Further, for any $\pi_i \in \mathrm{V}(\Gamma_k)$ we have that there is a shortest path of length $i-1 < k$ from π_i to e, so condition (ii) of Proposition 4.30 is also satisfied. □

This is all that is required for the result for Faber-Moore-Chen graphs. The same problem for the Gómez graphs was an open problem to which we now provide a solution. However, the work required will require significantly more detail and care over the next sections.

4.9 Paths in Gómez Graphs

In order to apply similar techniques to the case of Gómez graphs we must first begin by establishing terminology for the discussion of Gómez graphs. For a Gómez graph $\mathrm{WG}(\Pi_k, n)$ we shall be counting paths of length k and $k-1$ in the alphabet fixing subgraph $\Gamma_k = \mathrm{Cay}(\Pi_k, S_k)$ from each $\pi \in \mathrm{V}(\Gamma_k)$ with $e \to \pi$ to e. It would prove

cumbersome to use the notation of the alphabet fixing subgraphs as Cayley graphs, so we will continue to think of them as subgraphs of word graphs and associate with each of their vertices a word and each of the adjacencies a rule. Further, we shall ultimately deal with the cases of Gómez graphs defined for odd diameter and even diameter separately.

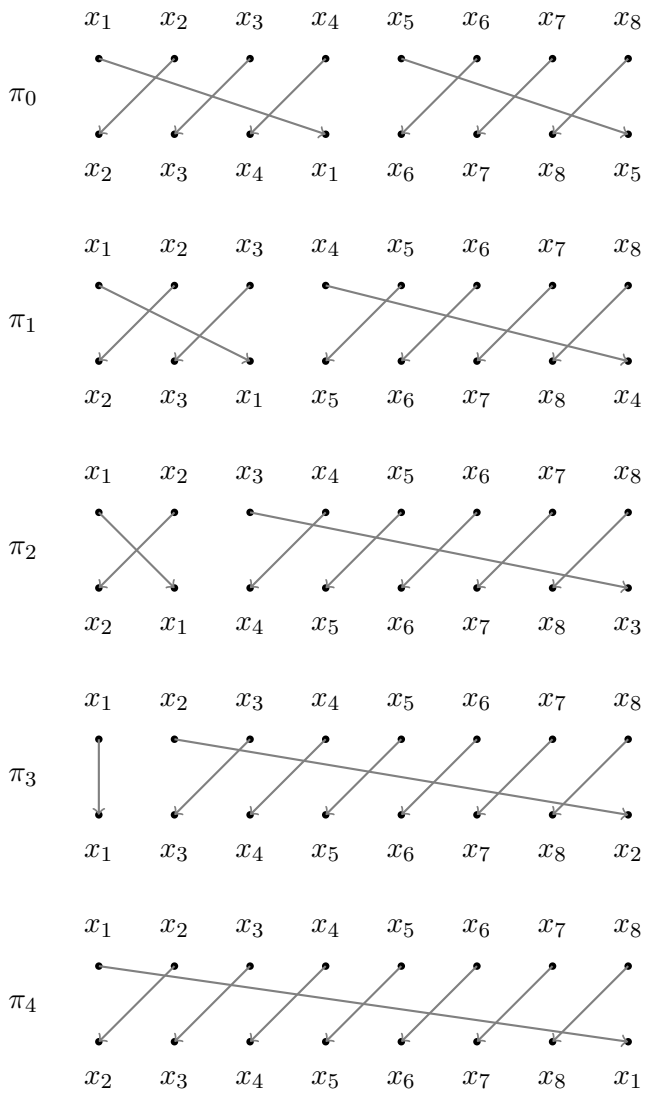
Throughout this section we shall consider the Gómez graph $\mathrm{GG}(d,k)$, which we shall denote as the word graph $G_d = \mathrm{WG}(\Pi_k, d)$. We shall denote the alphabet fixing subgraph of G_d as $\Gamma_k = \mathrm{Cay}(\Pi_k, S_k)$. We shall use our representation of Γ_k as a word graph rather than as a Cayley graph in our discussion, and shall now introduce a visual representation of the adjacencies and associated terminology. We illustrate with the example of Γ_8. We may define Γ_8 over the alphabet $B = \{1,2,3,4,5,6,7,8\}$. The vertices of Γ_8 are given by

$$\mathrm{V}(\Gamma_8) = \{x_1x_2x_3x_4x_5x_6x_7x_8 | x_i \in B, x_i = x_j \Leftrightarrow i = j\}.$$

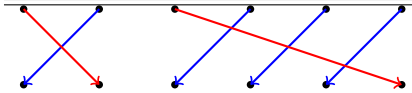
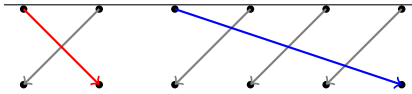
That is, the vertices of Γ_8 are all words of length 8 with letters in B and all letters distinct. The adjacencies of a vertex $x_1x_2x_3x_4x_5x_6x_7x_8 \in \mathrm{V}(\Gamma_8)$ are given as follows

$$x_1x_2x_3x_4x_5x_6x_7x_8 \rightarrow \begin{cases} x_2x_3x_4x_5x_6x_7x_8x_1 & \text{by } \pi_4, \\ x_1x_3x_4x_5x_6x_7x_8x_2 & \text{by } \pi_3, \\ x_2x_1x_4x_5x_6x_7x_8x_3 & \text{by } \pi_2, \\ x_2x_3x_1x_5x_6x_7x_8x_4 & \text{by } \pi_1, \\ x_2x_3x_4x_1x_6x_7x_8x_5 & \text{by } \pi_0, \end{cases}.$$

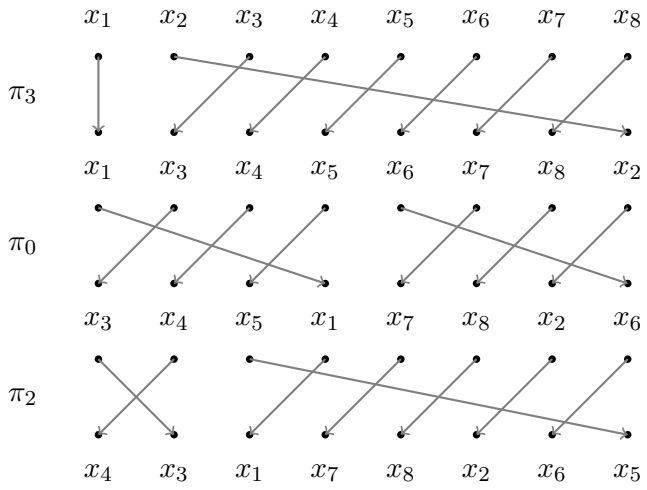
We shall visually represent these adjacencies with diagrams of the following form.



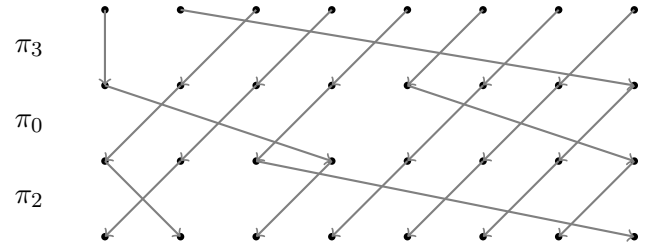
Within this visual representation, we label the following features.

Diagram	Red	Blue
	forward arrows	backward arrows
	left arrow	right arrow

We shall call the composition of adjacencies a *path* and represent it as in the following diagram.



In subsequent diagrams we may drop the explicit labelling of letters to present the same path in a more succinct manner, as in the example below.

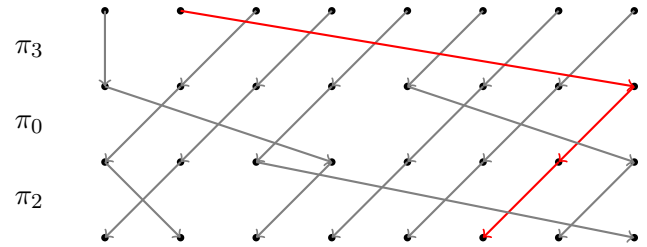


We now have enough definitions for our first lemma.

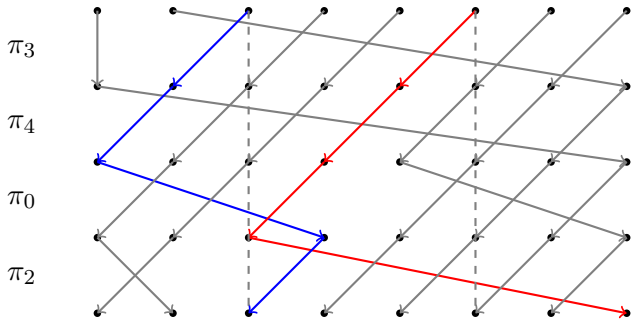
Lemma 4.33. *The number of right arrows in a path of length m is m, and the number of left arrows in a path of length m is less than or equal to m.*

Proof. Each of the rules π_i for $0 \leq i \leq k$ contains exactly one right arrow and either one or zero left arrows. □

In a path we shall use the *trail* from position i to mean the concatenation of consecutive arrows in our diagram beginning from the arrow at position i. In the following example we highlight the trail starting at position 2.



We shall call a trail *closed* if it begins and ends at the same position. Here we illustrate both a closed trail and a non-closed trail.



For a path $p = p_1 p_2 \dots p_n$, $p_j \in \Pi_k$, we shall call $p^i = p_i p_{i+1} \dots p_n p_1 p_2 \dots p_{i-1}$ the i^{th} rotation of p.

Lemma 4.34. *If the trail starting in position i in a path p is closed, then the trail starting at position $p_1(i)$ in p^2 is also closed.*

Proof. We have

$$\begin{aligned} p(i) = i \quad &\Leftrightarrow \quad (p_1 p_2 \dots p_n)(i) = i \\ &\Leftrightarrow \quad (p_2 p_3 \dots p_n)(p_1(i)) = i \\ &\Leftrightarrow \quad p_1((p_2 p_3 \dots p_n)(p_1(i))) = p_1(i) \\ &\Leftrightarrow \quad (p_2 p_3 \dots p_n p_1)(p_1(i)) = p_1(i) \\ &\Leftrightarrow \quad p^2(p_1(i)) = p_1(i). \end{aligned}$$

□

Corollary 4.35. *If the trail starting in position i in a path p is closed, then the trail starting at position $(p_1 p_2 \dots p_{j-1})(i)$ in p^j is closed.*

Proof. This is a trivial induction. □

In light of this corollary we will identify a closed trail with all of its images under rotation, and simply consider them to be the same trail.

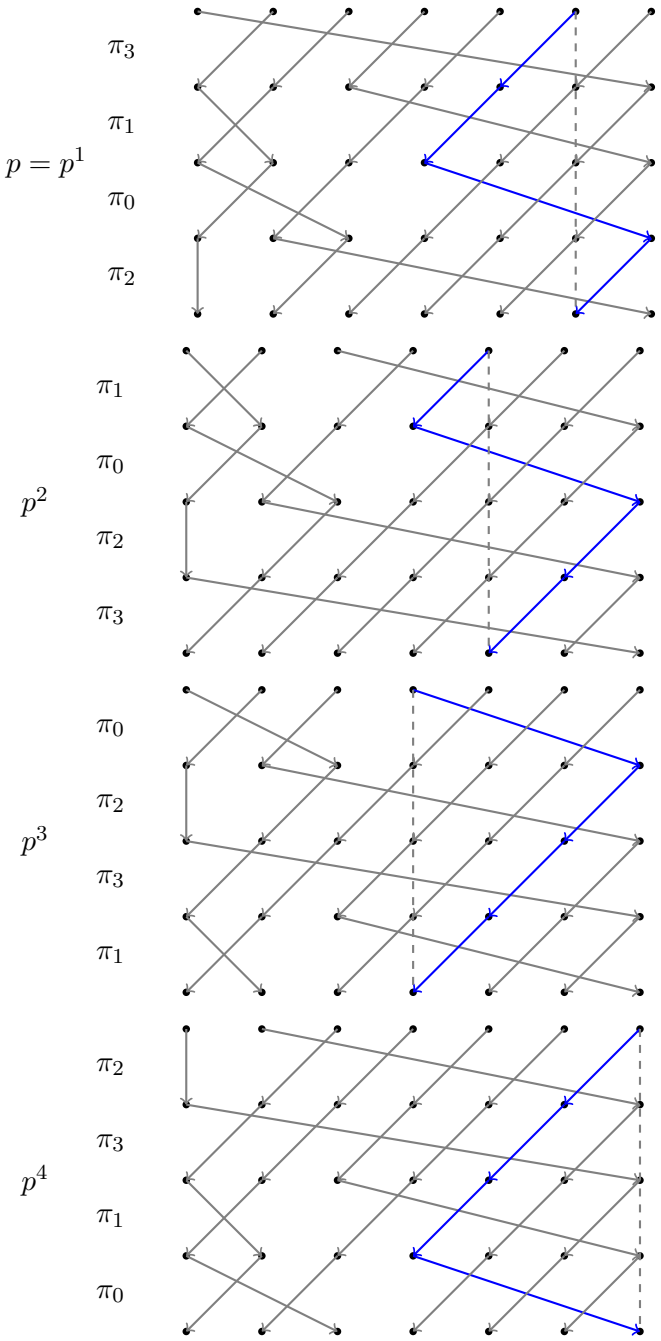
We shall call a path *closed* if the trails at each position in the path are closed.

Lemma 4.36. *There is a bijection between the closed trails of a path p and the closed trails of each of its rotations p^i.*

Proof. Consider a path p of length n and some $1 < i < n$. From Corollary 4.35 we have that a closed trail starting at any j in p corresponds to a closed trail starting at $(p_1 p_2 \dots p_{i-1})(j)$ in p^i. Hence there is a injective mapping from the closed trails of p to the closed trails of p^i. For the reverse, if we have a closed trail starting at j' in p^i we may define j such that $(p_1 p_2 \dots p_{i-1})(j) = j'$, and we may use Corollary 4.35 to

see there is a close trail in $(p^i)^(n-i) = p$ starting at $(p_i p_{i+1} \dots p_n)((p_1 p_2 \dots p_{i-1})(j)) = (p_1 p_2 \dots p_n)(j)$, hence there is an injective mapping from the closed trails of p^i to the closed trails of p. The result immediately follows. □

We illustrate closed trails in paths with the following example.



Corollary 4.37. *A path is closed if, and only if, each of its rotations is closed.*

Proof. This is an immediate consequence of Lemma 4.36. □

We have established basic notation and properties necessary for discussing paths of interest in Gómez graphs, and now describe our ultimate motivation before introducing further lemmas. In order to show that the Gómez graphs are subregular, and that they are alphabet stable, in the Gómez graph $\mathrm{GG}(d, k)$ we shall count the number of paths of length d from each π_i to e in the alphabet fixing subgraph Γ_k. These correspond to closed paths of length $k+1$, and closed paths in our above notation. We will use our above notation to count the number of closed paths of length $k+1$ from e to itself. We now introduce lemmas for this purpose.

Lemma 4.38. *Any closed trail in a path of length $k+1$ must contain at least two forward arrows.*

Proof. In a closed trail we have that the distance travelled forwards by forward arrows must be equal to the distance travelled backwards by backwards arrows. As the Gómez graphs are shift restricted, we have that each backwards arrow maps backwards exactly one space. In a trail of length $k+1$ with no forwards arrows there would be $k+1$ backwards arrows, and the trail would not be closed. In a trail of length $k+1$ with one forwards arrow there would be k backwards arrows, so if the trail were closed the forwards arrow would map k spaces forwards. However, the most any forward arrow maps forwards is in the rule π_k which contains one forwards arrow mapping $k-1$ spaces forwards. Hence, there is no closed trail in a path of length $k+1$ with either zero or one forwards arrows, and so any closed trail in such a path must have at least two forwards arrows. □

Lemma 4.39. *Any closed trail in a path of length $k+1$ whose only forward arrows are left arrows contains at least three left arrows.*

Proof. The furthest that can be mapped forwards by any left arrow occurs in the rule π_0 which maps forward $n-1$ spaces. If we have a trail of length $k+1$ which contains exactly two forward left arrows and no other forward arrows then there are $k-1$ backwards arrows in the trail. So the forwards arrows map $k-1$ spaces forwards. However, we have that we map forwards at most $2(n-1) < k-1$ spaces, and no such path exists. Therefore, combining with Lemma 4.38, in a closed trail of length $k+1$ where all forwards arrows are left arrows we see there must be at least three left arrows. □

Lemma 4.40. *Any closed trail in a path of length $k+1$ whose only forward arrows are right arrows contains exactly two right arrows.*

Proof. From Lemma 4.38 we know that any closed trail in a path of length $k+1$

which contains only right forwards arrows must contain at least two right forwards arrows. Therefore we must show that a closed trail in a path of length $k+1$ whose only forwards arrows are right arrows cannot contain three or more right arrows. Each right arrow maps forwards by at least n spaces, so in any closed trail containing at least three right arrows the total amount mapped forwards is at least $3n$. The total amount mapped backwards by such a trail is at most $k-2$. Hence, as amount mapped backwards must equal the amount mapped forwards we must have $k-2 \geq 3n$. However, we have $k \leq 2n+1$ and so $k-2 \leq 2n-1 < 3n$ so no such trail can exist. □

Lemma 4.41. *In a closed path of length $k+1$ there are at most three trails containing two right arrows.*

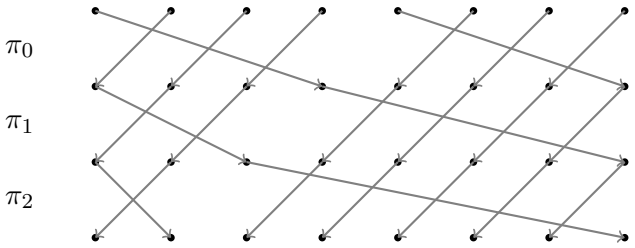
Proof. Suppose we have a closed path of length $k+1$ which has at least four closed trails containing two right arrows. By Lemma 4.33 we have that the path contains $k+1$ right arrows and at most $k+1$ left arrows, so there are at most $(k+1)-8 = k-7$ unaccounted for right arrows remaining in the path. Lemma 4.38 tells us that each trail in the path requires at least two forward arrows, and Lemma 4.39 tells us that if all forward arrows in a trail are left arrows then we require at least three left arrows. To minimise the number of forward arrows required for the closed trails we may assume as many right arrows as possible are in trails with left arrows. If all remaining right arrows occur in a trail with one left arrow, then there are $k-7$ trails containing a right and a left arrow, and at most $(k+1)-(k-7) = 8$ left arrows unaccounted for. We have now accounted for 4 closed trails with only right arrows and $k-7$ closed trails with a left and a right arrow. This leaves $k-(k-7)-4 = 3$ closed trails unaccounted for in the path. As there are no further right arrows unaccounted for, all of these trails contain only left forwards arrows, and by Lemma 4.39 require at least 9 left arrows. However, we have seen there are only 8 left arrows unaccounted for at most. Therefore no such closed path can exist, and a closed path of length $k+1$ can contain at most three trails containing two right arrows. □

Lemma 4.42. *In a path $p = p_1 p_2 \dots p_{k+1}$ of length $k+1$, if the trail starting at the right arrow of p_1 contains no further right arrows then it contains the left arrow of p_{k+1}.*

Proof. After p_1 the trail starting at the right arrow of p_1 is in position k. As the trail contains no further right arrows, whenever the trail is in a position $i > 1$ the next rule must give a backwards arrow in the trail, and hence the next position of the trail is

$i-1$. Therefore each p_{1+i} maps the trail from $k+1-i$ to $k-i$ for $1 \leq i < k$, leaving the trail at position 1 after rule p_k. Finally, this leaves the trail mapped forwards by the left arrow of rule p_{k+1}. □

In light of Lemma 4.42 we shall make the definition that if a path $p = p_1 p_2 \dots p_m$ of length m contains two consecutive rules p_i and p_{i+1} such that $p_i = \pi_j$ and $p_{i+1} = \pi_{j+1}$ we shall call the left and right arrows of p_i and p_{i+1} *paired* and refer to them together as a *pair*. We shall also allow the special case that for $p_i = p_m$ we shall consider $p_{i+1} = p_1$. For clarity we give diagrams showing pairing in paths.



Lemma 4.43. *If a closed trail of length $k+1$ contains both left and right arrows then it contains a pair and no other forward arrows.*

Proof. Suppose that p is a path containing a closed trail with both a left and a right arrow. Let q be some rotation of p such that a right arrow of the closed trail is in rule q_1 and such that the next forwards arrow in the trail is a left arrow. As the next arrow in the trail is a left arrow, we must have $(q_2 q_3 \dots q_i)(k) = 1$ for some i, with each q_j for $2 \leq j \leq i$ containing a backwards arrow in the trail and q_{i+1} containing a left arrow in the trail. As each backwards arrow in the trail maps backwards by one space, we have that $(q_2 q_3 \dots q_j)(k) = k+1-j$ for $1 \leq j \leq i$, and so we must have $i = k$. Therefore, the next left arrow in the trail is at position q_{k+1}, and hence only q_1 and q_{k+1} contain forward arrows of the trail and all other positions contain backward arrows. Finally, as the trail is closed we deduce that the right arrow in q_1 and the left arrow in q_{k+1} are a pair. □

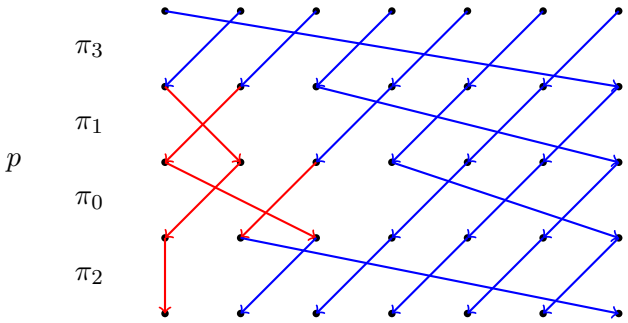
Lemma 4.44. *A closed trail in a path of length $k+1$ which contains right arrows either contains exactly two right arrows or contains a pair.*

Proof. If a closed trail in a path of length $k+1$ contains right arrows then either it contains both left and right arrows and so is a pair by Lemma 4.43 or it contains only right arrows and therefore exactly two right arrows by Lemma 4.40. □

Lemma 4.45. *If all right arrows in a path p of length $k+1$ are either in closed trails or are in pairs, then all pairs in p are in distinct closed trails.*

Proof. Consider an arbitrary right arrow in p and a rotation q of p which has that right arrow in position q_1. We aim to show that the trail starting with the right arrow of q_1 is a closed trail. We know that all right arrows in p are either in closed trails or in pairs by assumption. If we are in the first case then we are done, hence we assume that we are in the second case. After the rule q_1 the trail we are considering is at position k after each q_{1+i} the trail is in position $k-i$ until we encounter the next forward arrow in the trail. If the next forward arrow in the trail is a right arrow then either we are in a closed trail and are done or that right arrow is in a pair, however the second case cannot occur as we would encounter the second right arrow in the trail after a backwards arrow. Therefore, we can suppose that the next forward arrow in the trail is a left arrow. If this is the case, we encounter the arrow in position 1, which first occurs at rule q_{k+1}. Hence, this left arrow is paired with the right arrow in position q_1 and therefore we are in a closed trail. □

Altogether we are now in a position to easily deal with closed trails containing right arrows. We now continue our discussion and investigate the case of closed trails containing only left arrows. In order to characterise trails which only contain left arrows we will require further terminology. Within a permutation in a path we shall say that a trail is on the *left side* if it is contained in an arrow inside a cycle with containing a left arrow, and we will say that it is on the *right side* otherwise. We shall say that between two rules a trail *changes sides* to mean it goes from being contained in the left side to the right side or from the right side to the left side. Below we give a diagram to clarify the terminology.



Lemma 4.46. *It is only possible for a trail to move from the left to right side between two consecutive rules π_a and π_b in a path if $b > a$.*

Proof. For any rules $\pi_a, \pi_b \in \Pi_k$ with $b \leq a$ we have that all left arrows in π_a terminate at heads of left arrows in π_b. □

For the remainder of this section we shall consider paths $p = p_1 p_2 \dots p_m$ with the

property that if $p_i = \pi_a$ and $p_{i+1} = \pi_b$ then $a \geq b - 1$ (note that for $p_i = p_m$ we take $p_{i+1} = p_1$).

Lemma 4.47. *If p is closed, any trail which changes side contains a pair.*

Proof. For any closed trail, the number of times the trail changes from left to right must equal the number of times the trail changes from right to left. If a trail changes sides at some point we know that there is a point where the trail changes sides from left to right. We consider a rotation q of p where the closed trail changes sides from left to right between q_1 and q_2. From our assumption on p, we have that if $q_1 = \pi_a$ and $q_2 = \pi_b$ then $a \geq b - 1$. Applying Lemma 4.46 we have the further restriction that $b > a$, so we must have $b = a + 1$. This shows that $q_1 = \pi_a$ and $q_2 = \pi_{a+1}$. Finally, the only trail which changes side from left to right between q_1 and q_2 is the trail containing the left arrow of q_1 and the right arrow of q_2 which are in a pair. Hence the closed trail of p we are considering contains this pair. □

Corollary 4.48. *If p is closed, any trail which contains only left arrows is always on the left side.*

We now make a further definition. For a path p we shall define the *closure* of p to be p concatenated with itself the smallest number of times necessary to form a closed path. As any path p corresponds to a permutation, say π, we know that the permutation has some order a such that $\pi^a = e$. This order is the same as the number of times we must concatenate p with itself to form a closed path.

Lemma 4.49. *If p is a path in which all trails containing right arrows are closed, then all trails containing only left arrows are always on the left side.*

Proof. Let q be the closure of p. We can now apply Corollary 4.48 to q to deduce that all trails containing only left arrows in q are always on the left side. We also have that the trails containing only left arrows in q correspond to the trails containing only left arrows in p as all trails containing right arrows in p are closed. Hence we can deduce from the fact the trails containing only left arrows in q are always on the left side that the trails containing only left arrows in p are always on the left side, as the property of being on the left side only depends on the path at each i^{th} position, which are the same for p and q for all positions of p. □

Lemma 4.50. *If p is a path where all trails containing right arrows are closed, and the trails starting at positions $a_1, a_2, \ldots a_m$ are all trails whose only forwards arrows are left arrows, and there are c left arrows in total in these trails, then p maps a_i to a_{i-m} where subscripts are considered modular.*

Proof. This is provable by a trivial induction. First, as all trails other than those starting at each a_i are closed, we see that p maps each a_i to some a_j. Now, as all the trails are always on the left side, only two things may happen at each rule: either all trails are mapped backwards one space by backward arrows, and thus their left to right order is preserved; or the trail on the far left is mapped by a left arrow and becomes the trail on the far right whilst all other trails are mapped backwards one space by backward arrows. The latter case happens exactly m times. Hence the left right ordering of the trails starting at $a_1, a_2, \ldots, a_m$ is cycled m times. □

Corollary 4.51. *If a path p has all trails with right arrows closed, and contains exactly two trails whose only forward arrows are left arrows, and those trails contain an even number of left arrows, then the path p is closed.*

Proof. Letting $2m$ be the number of left arrows in trails containing only left arrows, we may use the previous lemma to show that a_1 gets mapped to $a_{1-2m} = a_1$ and a_2 gets mapped to $a_{2-2m} = a_2$. Therefore the trails starting at a_1 and a_2 are closed. □

We have now established sufficient lemmas and terminology to help us approach the problem of counting paths of certain length in Gómez graphs. In order to precede, we will now need to consider separately the case of Gómez graphs with odd diameter and Gómez graphs with even diameter. We shall start with the former case as it is the simpler case.

4.9.1 The Odd Case

We now consider the case of counting closed paths in Gómez graphs of odd diameter. In this section we will consider the Gómez graph $G = \mathrm{GG}(d, k)$ where $k = 2n + 1$. We will take $G = \mathrm{WG}(\Pi_k, d)$ where $\Pi_k = \{\pi_0, \pi_1, \ldots, \pi_n\}$ with alphabet fixing subgraph Γ_k as previously. In this section we will count all paths of length $k + 1$ from e to e in Γ_k, which correspond to closed paths of length $k + 1$ as described in the previous section. Throughout we shall assume $p = p_1 p_2 \ldots p_{k+1}$ is such a closed path.

Lemma 4.52. *If $p_1 = \pi_0$, then $p_{n+1} = \pi_0$, and the trail beginning at position $n + 1$ contains two right arrows.*

Proof. We consider the trail starting with the right arrow of p_1. As this trail is closed, from Lemma 4.44 we have that the trail either contains two right arrows or a pair. Therefore we know that the trail maps backwards $k - 1$ spaces, and therefore, as the right arrow in p_1 maps forwards n spaces, the other forwards arrow maps forwards $(k - 1) - n = n$ spaces. The most any left arrow maps forward is $n - 1$ spaces, so the

other arrow must be a right arrow occurring in rule π_0. To see that this occurs in p_{k+1} we simply observe that each rule p_i for $1 < i < k+1$ maps the trail back one space. □

Corollary 4.53. *There are at most 6 occurrences of rule π_0 in the path p.*

Proof. This is a combination of the previous lemma and Lemma 4.41. □

Lemma 4.54. *If $p_1 = \pi_i$ for some $i \geq 1$, then $p_{k+1} = \pi_{i-1}$.*

Proof. Consider the trail starting with the right arrow of p_1. If this trail contains a left arrow we may apply Lemma 4.42 and we are done. Otherwise, Lemma 4.40 shows that there is exactly one other right arrow in the trail. Therefore we see that the distance mapped backwards in the trail is $k-1$, and the distance mapped forwards by the right arrow of p_1 is $n+i$. Therefore, the other right arrow maps forwards $(k-1)-(n+i) = n-i$ spaces. However, all right arrows map forwards at least n spaces, and the trail cannot contain two right arrows. □

Corollary 4.55. *If $p_i = \pi_j$ for $j \neq 0$, then $p_{i-1} = \pi_{j-1}$.*

Proof. Let q be the rotation of p where p_i is q_1, then apply Lemma 4.54. □

Lemma 4.56. *In the path p we have $p_i = p_{i+(n+1)}$.*

Proof. First, if $p_i = \pi_0$ we choose the rotation $q = p^{(k+1)-i}$ of p such that $q_1 = p_i$, then we apply Lemma 4.52 to deduce that $p_{i+(n+1)} = \pi_0$. For $p_i = \pi_j$ we again consider the rotation $q^{(k+1)-1}$ of p, and repeatedly apply Corollary 4.55 to show that $q_{1+i} = \pi_{j-i}$ for $0 \leq i \leq j$. We then deduce that $q_{(n+1)+j} = \pi_0$. Now, suppose that $q_{n+j} = \pi_c$. If $\pi_c = \pi_0$ then $q_{1+(j-1)} = \pi_0$, contradicting the fact $q_{1+(j-1)} = \pi_1$, and if $c \geq 1$ then we may apply Corollary 4.55 and the fact $q_{(n+1)+j} = \pi_0$ to deduce that $c = 1$. Repeatedly applying this observation gives us that $q_{1+i} = q_{(n+1)+i}$ for all $0 \leq i \leq j$. Altogether we have shown $p_i = p_{i+(n+1)}$ in all cases. □

Now suppose that $p = \pi_{a_1}\pi_{a_2}\ldots\pi_{a_{k+1}}$ is a closed path of length k. We now characterise the sequence $a_1, a_2, \ldots, a_{k+1}$ and use our characterisation to count all such possible sequences for each different possible first member a_1.

Proposition 4.57. *A sequence $a_1, a_2, \ldots, a_{k+1}$ corresponds to a closed path if, and only if, the following properties hold*

i) $a_i = a_{(n+1)+i}$;

ii) if $a_i = j$ for $j > 0$ then $a_{i+1} = j - 1$;

iii) there are at most 6 distinct i such that $a_i = 0$.

Proof. We first show that these are necessary conditions for the path p to be closed. We have that property (i) is a consequence of Lemma 4.56; property (ii) is a consequence of Corollary 4.55; and that property (iii) is a consequence of Lemma 4.41 (that there are at most three trails containing two right arrows in a closed path) and Lemma 4.52.

We now show that these conditions are sufficient. Suppose that $\langle a_i \rangle$ is a sequence with these properties, and $p = p_1 p_2 \dots p_{k+1} = \pi_{a_1} \pi_{a_2} \dots \pi_{a_{k+1}}$ is the corresponding path. As shown in the proof of Lemma 4.52, if $p_i = \pi_0$ and $p_{i+(n+1)} = \pi_0$ then the right arrows of p_i and $p_{i+(n+1)}$ are in the same closed trail. For all other rules, we have some $p_i = \pi_j$ for $j > 0$, and we must have $p_{i+1} = \pi_{j-1}$. Hence, for all rules $p_i = \pi_j$ in p for $j > 0$ we have that the right arrow of p_i is in a pair with the left arrow of p_{i+1}. We can apply Lemma 4.45 as we have shown that all right arrows are either in closed trails or in pairs. Altogether, this shows that each pair of rules $p_i = \pi_0$ and $p_{i+(n+1)} = \pi_0$ corresponds to a closed trail containing the right arrows of both rules, and that for all other rules $p_i = \pi_j$, $j > 0$, the right arrow of p_i corresponds to another distinct closed trail. We now consider different cases based on how many rules $p_i = \pi_0$ there are in our path. We note that there are an even number of rules π_0 in our path; that there aren't more than 6 such rules by Lemma 4.41; and from Corollary 4.55, the fact the paths we consider are length $k + 1$ and the rules π_j satisfy $j \leq n$ we have that there are at least 2 rules π_0 in our path. Now we consider the cases of 2, 4 or 6 rules π_0 in our path.

i) Suppose there are two rules p_i such that $p_i = \pi_0$. In this case we have accounted for 1 closed trail in right arrows from rules of the form $p_i = 0$, and $(k + 1) - 2 = k - 1$ further closed trails corresponding to the other right arrows in the path. Altogether we have accounted for k closed trails, so as there are only k trails in the path the path must be closed.

ii) Suppose there are four rules p_i such that $p_i = \pi_0$. In this case we have accounted for 2 closed trails corresponding to the right arrows in rules of the form $p_i = \pi_0$, and $(k + 1) - 4 = k - 3$ further closed trails corresponding to the other right arrows in the path. Altogether we have accounted for $k - 1$ closed trails, so as there are only k trails in the path this means there is only 1 trail left to account for. However, as there is only one trail left and all others are known to be closed this final trail must start and end in the same place, and must also be closed.

iii) Suppose there are six rules p_i such that $p_i = \pi_0$. In this case we have accounted for 3 closed trails with right arrows in rules of the form $p_i = \pi_0$. All other rules of the form $p_i = \pi_j$ correspond to a right arrow which is contained in a pair and thus corresponds to a closed trail. Therefore, this gives $(k+1) - 6 = k - 5$ closed trails corresponding to right arrows in pairs, and 3 closed trails containing only right arrows. Hence, we have accounted for all but $k - (k-5) - 3 = 2$ of the trails of p. We must have that the remaining trails in our path only use left arrows. We cannot have a rule π_k in p as there are 6 rules π_0 in p, so all rules have both a left and right arrow and there must be 6 left arrows unaccounted for in p. Now applying Corollary 4.51 we get the result. □

Altogether this gives us a characterisation for the closed paths of length $k+1$ in terms of sequences with particular properties. We shall now call a sequence $a_1 a_2 \dots a_{n+1}$ a *τ-sequence* if

i) all a_i satisfy $a_i \geq 0$;

ii) if $a_i > 0$ then $a_{i-1} = a_i - 1$;

iii) there are at most three i such that $a_i = 0$;

iv) if $a_1 a_2 \dots a_{n+1}$ is a τ-sequence, then $a_n a_1 a_2 \dots a_{n-1}$ must also be a τ-sequence.

We may now restate the previous proposition as follows.

Proposition 4.58. *A path $p = \pi_{a_1} \pi_{a_2} \dots \pi_{a_{k+1}}$ is closed if, and only if, $a_i = a_{(n+1)+i} = b_i$ for $1 \leq i \leq n+1$ and b_i is a τ-sequence.*

We now aim to count the number of different τ-sequences $\langle a_i \rangle$ for each possible value of a_1. We shall use the notation $\tau(n, \alpha, \beta)$ to indicate the number of τ-sequences of length n such that $a_1 = \alpha$ and $a_n = \beta$, and the notation $\tau(n, \alpha)$ to indicate the number of τ-sequences of length n with $a_1 = \alpha$.

Lemma 4.59. *For $n > 1$, $\tau(n, 0, 0) = n - 1$.*

Proof. We begin with the observation that, in any τ-sequence, if $a_k = 0$ and $a_{k+j} \neq 0$ for some range of j then we may repeatedly apply properties (i) and (ii) to deduce that $a_{k+j} = j$ for all j in the range. In particular, all a_{k+j} are uniquely defined.

Now suppose that $a_1 a_2 \dots a_n$ is a τ-sequence with $a_1 = a_n = 0$. First, suppose that there is no j such that $a_j = 0$ and $1 < j < n$. If this is the case then $a_j = j - 1$ and there is exactly one τ-sequence with this property.

Now suppose that there is some k such that $1 < k < n$ and $a_k = 0$. By property (iii) there are no further values $j \notin \{1, k, n\}$ such that $a_j = 0$. As a result for $1 < j < k$ we must have $a_j = j - 1$ and for $k < j < n$ we must have $a_{k+j} = j$. Hence there is exactly one τ-sequence with $a_k = 0$ for each possible value of k. This gives $n - 2$ possible τ-sequences.

In total, this gives us $n - 1$ possible τ-sequences where $a_1 = a_n = 0$, and so $\tau(n, 0, 0) = n - 1$. □

Lemma 4.60. *For $1 < i \leq n$, we have $\tau(n, 0, n - i) = i - 1$.*

Proof. Suppose that $a_1 a_2 \dots a_n$ is a τ-sequence with $a_1 = 0$. If $a_n = \alpha > 0$, then we see that $a_1 a_2 \dots a_n$ is a τ-sequence of length n if, and only if, $a_1 a_2 \dots a_{n-1}$ is a τ-sequence of length $n - 1$. Therefore we have $\tau(n, 0, \alpha) = \tau(n - 1, 0, \alpha - 1)$ for all $\alpha > 0$. We may repeatedly apply this observation to show that $\tau(n, 0, \alpha) = \tau(n - \alpha, 0, 0)$, which shows $\tau(n, 0, n - i) = \tau(n - (n - i), 0, 0) = \tau(i, 0, 0) = i - 1$. □

Proposition 4.61. *For $1 \leq i \leq n$, $\tau(n, n - i) = (i^2 - i + 2)/2$.*

Proof. We proceed by induction on i. We start with the case $i = 1$. To calculate $\tau(n, n - 1)$, let $a_1 a_2 \dots a_n$ be a τ-sequence with $a_1 = n - 1$. By property (iv) we equivalently have that $a_2 a_3 \dots a_n a_1$ is a τ-sequence. Now we may repeatedly apply properties (i) and (ii) to show that $a_i = i - 1$, and that there is a unique possible τ-sequence. Hence $\tau(n, n - 1) = 1$.

We suppose $i = k$ and we have the hypothesis given for $i = k - 1$. Let $a_1 a_2 \dots a_n$ be a τ-sequence with $a_1 = (n - k)$. By property (ii) we have that either $a_2 = 0$ or $a_2 = n - k + 1$. In the first case we may rotate to get a τ-sequence beginning with 0 and ending with $n - k$. In the second case we may rotate to get a τ-sequence beginning with $n - (k - 1)$. This gives

$$\begin{aligned} \tau(n, n - k) &= \tau(n, 0, n - k) + \tau(n, n - (k - 1)) \\ &= k - 1 + ((k - 1)^2 - (k - 1) + 2)/2 \\ &= (k^2 - k + 2)/2. \end{aligned}$$

□

Now combining Proposition 4.58 and Proposition 4.61 we get the following proposition.

Proposition 4.62. *Letting Γ_k be the alphabet fixing subgraph $\mathrm{Cay}(\Pi_k, S_k)$ of the Gómez graph $\mathrm{WG}(\Pi_k, d)$, there are $(i^2 - i + 2)/2$ paths of length k from each π_i to e.*

Proof. This is a combination of the fact the closed paths of length $k+1$ correspond to paths of length $k+1$ from e to e in Γ_k, and the use of Proposition 4.58 and Proposition 4.61 to count each of these paths beginning with different symbols. □

We are now able to prove our main proposition.

Proposition 4.63. *For $k = 2n+1$ and all $m \geq k$, the Gómez graphs $G_m = \mathrm{WG}(\Pi_k, m)$ satisfy $\mathrm{Aut}(G_m) \cong S_m$.*

Proof. We apply the test of Proposition 4.30. We consider the alphabet fixing subgraph Γ_k of G_m. For each π_i, π_j such that $e \to \pi_i$ and $e \to \pi_j$ we have from Proposition 4.62 that there are $(i^2 - i + 2)/2$ paths of length k from π_i to e and there are $(j^2 - j + 2)/2$ paths of length k from π_j to e. Therefore, there are the same number of paths from π_i to e and π_j to e of length k if, and only if, $i = j$ (given that $0 \leq i, j \leq k$). Each pair π_i and π_j satisfy property (i) of Proposition 4.30. For all i except $i = 0$ we have $(i^2 - i + 2)/2 > 1$, hence all π_i except π_0 satisfy property ii of Proposition 4.30. For the remaining vertex π_0 we have that π_0 is a k-cycle and so $\pi_0^k = e$, so there is a path of length $k-1$ from π_0 to e and π_0 also satisfies property ii. Therefore Γ_k satisfies the conditions of Proposition 4.30 and we have $\mathrm{Aut}(G_m) \cong S_m$. □

4.9.2 The Even Case

In this section we shall deal with the extremal Gómez graphs of even diameter. Throughout this section we let $k = 2n$ for $k > 1$. We shall consider an arbitrary closed path $p = p_1 p_2 \dots p_{k+1}$.

Lemma 4.64. *If $p_1 = \pi_0$, then $p_{n+2} = \pi_1$, and the closed trail starting at $n+1$ contains two right arrows.*

Proof. The closed trail starting at $n+1$ is the trail containing the right arrow of p_1, therefore at rule p_2 the trail is in position k. If we assume that there are no further right arrows in this trail, then Lemma 4.42 tells us that this trail contains the left arrow of p_{k+1}, and as the trail is closed we know that this left arrow maps from position 1 to position $n+1$. However, the furthest any left arrow maps is from position 1 to position n in rule π_0, and so no such left arrow exists. Therefore, the trail containing the right arrow of p_1 must contain another right arrow, and by Lemma 4.40 it must contain exactly two right arrows. The second right arrow must map $(k-1) - (n+1) = n$ spaces forwards, and must therefore be the right arrow

from rule π_1. This rule must occur in the trail after being mapped n spaces backwards after p_1, and hence must occur in rule p_{n+2}. □

Corollary 4.65. *The rule π_0 occurs at most three times in p.*

Proof. This is a result of the combination of Lemma 4.41 which states that a closed path of length $k+1$ contains at most three trails containing two right arrows and Lemma 4.64. □

Lemma 4.66. *If $p_1 = \pi_1$, then either $p_{n+1}\pi_0$ or $p_{k+1} = \pi_0$.*

Proof. We consider the trail starting with the right arrow of p_1. If the trail contains a further right arrow, then again Lemma 4.40 tells us there is exactly one further right arrow and we may again apply the previous logic to deduce that the other right arrow is in the rule π_0 in rule p_{n+1}. Otherwise, we may apply Lemma 4.42 to deduce that the other left arrow in the trail is in a pair with the right arrow of p_1 and thus $p_{k+1} = \pi_0$. □

Lemma 4.67. *If $p_1 = \pi_i$ for some $i \geq 2$ then $p_{k+1} = \pi_{i-1}$.*

Proof. Consider the closed trail starting with the right arrow of p_1. If the trail contains two right arrows, then by Lemma 4.40 there are exactly two right arrows, and therefore the second right arrow maps forward $(k-1)-(n-i) = n+i$ spaces. However, the most any right arrow maps forward is n spaces in the rule π_0. Hence no such right arrow exists and the closed trail starting with the right arrow of p_1 must contain only one right arrow. Therefore, we may apply Lemma 4.42 to deduce that there is one other forwards arrow in the trail which is a left arrow paired with the right arrow of p_1, and we see $p_{k+1} = \pi_{i-1}$. □

Proposition 4.68. *The path $p = p_{a_1}p_{a_2}\dots p_{a_{k+1}}$ is closed if, and only if, $a_1, a_2, \dots a_{k+1}$ is a sequence with the following properties.*

i) $0 \leq a_i \leq k$ *for all i;*

ii) there are at most three i such that $a_i = 0$;

iii) if $a_i = 0$ then $a_{i+(n+1)} = 1$;

iv) if $a_i = j$ for $j > 0$ then $a_{i+1} = j-1$ (in the special case that $i = k+1$ we take a_1 for a_{i+1});

Proof. First, suppose that $p = p_{a_1} p_{a_2} \dots p_{a_{k+1}}$ is a closed path. We trivially have property (i). Property (ii) follows from Lemma 4.65. Property (iii) follows from Lemma 4.64. Property (iv) follows from Lemma 4.67.

Now suppose $a_1 a_2 \dots a_{k+1}$ is a sequence with these properties. For each $a_i = 0$ in the sequence we have $a_{i+(n+1)} = 1$, so if we consider the rotation $q = p^{(k+1)-(i+1)}$ of p which puts rule $p_i = \pi_{a_i}$ at the beginning of the path we have that $q_1 = \pi_0$ and $q_{n+2} = \pi_1$. We cannot have that $q_{n+1} = \pi_0$ as that would imply $q_1 = \pi_1$. Therefore the trail starting from the right arrow of q_1 is mapped backwards by each of the rules q_j for $1 < j < n + 2$, and then is mapped forwards by the right arrow of rule q_{n+2}. After being mapped forwards by q_{n+2}, the trail is mapped backwards by all rules up to q_{k+1}, and we see it ends in position $n + 1$ and we see that the trail is closed. For all other right arrows in p occurring in some rule say $p_i = \pi_{a_i}$ we have $p_{i+1} = \pi_{a_{i+1}}$, and hence the right arrow of p_i is in a pair with the left arrow of p_{i+1}. Therefore all right arrows are either in closed trails or are in pairs, and we may apply Lemma 4.45. Finally we follow the same logic as Proposition 4.57 and we are done. □

In light of this lemma, for $k = 2n$, we now call a sequence $a_1 a_2 \dots a_{k+1}$ a σ-sequence if it has the following properties.

i) $a_i \geq 0$;

ii) if $a_i = 0$ then $a_{i+(n+1)} = 1$;

iii) if $a_i = 1$ then either $a_{i-1} = 0$ or $a_{i+k} = 0$;

iv) if $a_i > 0$ then $a_{i-1} = a_i - 1$;

v) there are at most three i such that $a_i = 0$;

vi) if $a_1 a_2 \dots a_{k+1}$ is a σ-sequence then $a_{k+1} a_1 a_2 \dots a_k$ is also a σ-sequence.

We may now rephrase Proposition 4.68 as follows.

Proposition 4.69. *A path $p = p_{a_1} p_{a_2} \dots p_{a_{k+1}}$ is closed if, and only if, $a_1, a_2, \dots, a_{k+1}$ is a σ-sequence.*

As these sequences aren't as readily visualisable from their description as τ-sequences we give some examples for $n \in \{9, 11\}$.

$n = 9$	$n = 11$
012341234	01234512345
010121212	01012312123
012011231	01201212312
001231123	01230112341
001011121	00123411234
001121101	00101211212
011011011	00120111231
000121112	00112311012
	00121211201
	01010112121
	01001210112
	00012311123

We immediately notice from our table that the 0s and 1s always appear in groups of the following forms

$$01\underbrace{\ldots}_{n-1}1\underbrace{\ldots}_{n-1}, \quad 001\underbrace{\ldots}_{n-2}11\underbrace{\ldots}_{n-2}, \quad \text{or} \quad 0001\underbrace{\ldots}_{n-3}111\underbrace{\ldots}_{n-3},$$

We shall call these patterns *01-groups*. We aim to show that each 0 or 1 in a σ sequence occurs in a unique 01-group (i.e. that 01-groups do not overlap). In the following, suppose that $a_1 a_2 \ldots a_{k+1}$ is a σ-sequence with $a_1 = 0$ and $a_{k+1} \neq 0$.

Lemma 4.70. *There is some $1 \leq \alpha \leq 3$ such that for $1 \leq i \leq \alpha$ we have $a_i = 0$, $a_{i+(n+1)} = 1$ and $a_{\alpha+1} = 1$.*

Proof. Let α be the largest number such that $a_i = 0$ for all $1 \leq i \leq \alpha$. From property (v) we have that $\alpha \leq 3$. From property (i) we have that $a_{\alpha+1} \geq 0$, and by definition of α we have $a_{\alpha+1} \neq 0$ hence we have $a_{\alpha+1} > 0$. From property (iv) we have, as $a_\alpha = 0$ and $a_{\alpha+1} > 0$ that we must have $a_{\alpha+1} = 1$. Finally, from the fact $a_i = 0$ for $1 \leq i \leq \alpha$ and property ii we have that $a_{i+(n+1)} = 1$ for $1 \leq i \leq \alpha$. □

Corollary 4.71. *Every 0 in a σ-sequence is in a unique 01-group.*

Proof. Consider a σ-sequence with $a_i = 0$ for some i. From property (vi) we may consider a rotation of $\langle a_j \rangle$ which moves this 0 from position i to position 1, and then possibly further to position 2 or 3 until $a_{k+1} \neq 0$. Then we may apply the previous lemma. □

Lemma 4.72. *Every 1 in a σ-sequence is in a unique 01-group.*

Proof. From property (iii) we have two possibilities if $a_i = 1$. In the first possibility we have that $a_{i-1} = 0$, and thus $a_{i+n} = 1$, so the two possibilities of property (iii) are mutually exclusive. In this possibility we may use Lemma 4.70 with $a_{i-1} = 0$ to find the 01-group of a_i. In the second possibility, we may use Lemma 4.70 with $a_{i+n} = 0$ to find the 01-group of a_i. □

Now we let $\sigma(i, k+1)$ where $k = 2n$ be the number of σ-sequences of length $k+1$ with $a_1 = i$.

Lemma 4.73. $\sigma(n, k+1) = 2$.

Proof. If $a_1 = n$ in a sequence, then by property (vi) we may consider a rotation of $\langle a_j \rangle$ such that $a_n = n$. Repeatedly applying property (iv) we may show that $1 \leq i \leq n$ that $a_i = i$. For $2 \leq i \leq n$ we have that $a_i > 1$ and hence we have a block of $n-1$ consecutive numbers not in a 01-group. Therefore, the only 01-group that can be in the sequence is $01\underbrace{\ldots}_{n-1}1\underbrace{\ldots}_{n-1}$. As $a_1 = 1$, and each occurrence of a 1 is in a 01-group, we must have that this 01-group is in our sequence and no other 01-group is in our sequence. We may now rotate our sequence again so that $a_1 = 0$. Now repeatedly applying property (iv) noting that all unknown a_i satisfy $a_i > 1$ we may deduce that $a_{i+1} = i$ and $a_{n+1+i} = i$ for all $2 \leq i \leq n$, and this is the only σ-sequence containing n up to rotation. Finally, we note that there are two distinct rotations of this sequence such that $a_1 = n$, giving us that $\sigma(n, k+1) = 2$. □

Lemma 4.74. $\sigma(0, k+1) \geq 3$.

Proof. For $n \geq 3$, we consider the σ-sequence with $a_1 = a_2 = a_3 = 0$, $a_4 = a_{n+2} = a_{n+3} = a_{n+4} = 1$ and $a_{3+i} = a_{n+3+i} = i$ for $2 \leq i \leq n-2$. This sequence may be rotated in to give $a_1 = 0$ in three different ways. Hence, in this case we have $\sigma(0, k+1) \geq 3$.

For $n = 2$ we consider the σ-sequences 00111, 01110 and 01212 to see that $\sigma(0, k+1) \geq 3$. □

Lemma 4.75. $\sigma(i, k+1) < \sigma(i-1, k+1)$ *for* $1 < i \leq k$.

Proof. Consider the map ϕ which takes a σ-sequence $a_1 a_2 \ldots a_{k+1}$ to $a_{k+1} a_1 a_2 \ldots a_k$. If $a_1 = i$ then $a_{k+1} = i - 1$ by property (iv), so we see ϕ is an injective map from σ-sequences starting with i to those starting with $i-1$. Hence, to show that $\sigma(i, k+1) < \sigma(i-1, k+1)$ we need only find a σ-sequence with $a_1 = i-1$ and $a_2 \neq i$.

For $i \leq n-1$, the sequence $a_1 = 0, a_2 = a_{n+2} = 1$, $a_{i+1} = 0, a_{i+2} = a_{i+k+2} = 1$ and all other a_j satisfying $a_j = a_{j-1} + 1$ is a σ-sequence with $a_i = i - 1$ and $a_{i+1} = 0 \neq i$. Therefore, by property (vi), we can take a rotation of $a_1 a_2 \dots a_{k+1}$ such that $a_1 = i - 1$ and $a_2 \neq i$.

For $i = n$ we consider the sequence $a_1 = 0$, $a_2 = a_{n+2} = 1$, $a_{n-1} = 0$, $a_n = 1$ and $a_{k+1} = 1$, and all other a_j satisfying $a_j = a_{j-1} + 1$. We see this is a σ-sequence in which $a_k = i - 1$, and $a_{k+1} = 1 \neq i$. Hence again by property (vi) we take a rotation of this σ-sequence with $a_1 = i - 1$ and $a_2 = 0 \neq i$. □

We now introduce a lemma concerning paths of length k rather than $k + 1$, this will become useful to show that an automorphism of Γ_k fixing e cannot interchange π_0 or π_n with any other π_i.

Lemma 4.76. *If p is a closed path of length k, no rule π_i where $0 < i < n$ may occur in p.*

Proof. Suppose that p is a path of length k containing some rule π_i with $0 < i < k$. We may rotate p as necessary to consider such a path in which $p_1 = \pi_i$. Now consider the trail starting with the right arrow of $p_1 = \pi_i$. This arrow maps forward $(n-1) + i$ spaces. If this trail contains another right arrow, then the total distance mapped forward is at least $2(n-1) + 1 > k - 2$, but the total distance mapped backwards by the trail is at most $k - 2$. Therefore this trail cannot contain another right arrow. Therefore, this trail must contain a left arrow. This can only happen after the first j such that $(p_2 p_3 \dots p_j)(k) = 1$, but we know that each p_i maps the trail backwards one space, and hence this first happens for $j = k$, leaving no space for a left arrow in the trail. □

Finally, we combine these lemmas to prove the following theorem.

Proposition 4.77. *The Gómez graph $G_d = \mathrm{GG}(d, k) = \mathrm{WG}(\Pi_k, d)$ satisfies $\mathrm{Aut}(G_d) = S_d$.*

Proof. Again we apply Proposition 4.30. We have shown that in the alphabet fixing subgraph Γ_k of $\mathrm{WG}(\Pi_k, d)$ that the paths of length $k + 1$ from e to e correspond to σ-sequences. From Lemma 4.75 we see that for $1 \leq i < j < n$ there are more paths of length k from π_i to e than there are from π_j to e, so π_i and pi_j satisfy condition (i) of Proposition 4.30. For π_0 and π_n we have that π_0 is a k-cycle and π_n is two n-cycles, so we must have $\pi_0^k = \pi_n^k = e$. From Lemma 4.76 we know that there is no path of length $k - 1$ from π_i to e for $0 < i < n$. Therefore, for $0 < i < n$ and $j \in \{0, n\}$ we

have that π_i and π_j satisfy condition (i) of Proposition 4.30. For π_n from Lemma 4.73 we have that there are two paths of length k from π_n to e, and for π_0 from Lemma 4.74 we have that there are at least three paths of length k from π_0 to e, so π_0 and π_n satisfy condition (i) of Proposition 4.30. Therefore, for any $0 \leq i, j \leq n$ where $i \neq j$ we have that π_i and π_j satisfy condition (i) of Proposition 4.30.

Finally, from Lemma 4.73, Lemma 4.74 and Lemma 4.75 we have that there are always at least two paths of length k from any π_i to e. As a result we see each π_i satisfies condition (ii) of Proposition 4.30. □

4.10 Problems In Other Cases

In our treatment of the Gómez graphs we have been careful to provide a definition of the Gómez graphs which only covers the extremal Gómez graphs for given degree and diameter. However, in the work in which the Gómez graphs originally appeared additional graphs were also allowed in the definition. These additional graphs corresponding to the following word graphs in our notation $\mathrm{GGE}(d, k, c) = \mathrm{WG}(\Pi_{k,c}, d - \lfloor k/2 \rfloor - c)$ where $\Pi_{k,c} = \{\pi_0, \pi_1, \pi_2, \ldots, \pi_{\lfloor k/2 \rfloor + c}\}$, and $\pi_i = (1\ 2\ \ldots\ (\lfloor k/2 \rfloor - i + c + 1))((\lfloor k/2 \rfloor - i + c + 2)\ \ldots\ k)$. Informally we may think of $\mathrm{GGE}(d, k, c)$ as being the Gómez graph $\mathrm{GG}(d, k)$ of degree d and diameter k with c additional alphabet fixing rules added to the set Π_k corresponding to the next c rules as the divison between the left cycle and right cycle of each rule moves to the right.

When considering these additional graphs, the argument we have given seems unsatisfying as it is not immediately obvious that it can't be expanded to cover all of these graphs. However, we shall now give some computed examples to show that any attempt to count the same paths in these addtional cases of graphs $\mathrm{GGE}(d, k, c)$ for parameters $c > 0$ will not serve our purposes. In the following table we give sample values for numbers of paths of length k from π_i to e in the alphabet fixing subgraphs of $\mathrm{GGE}(d, k, c)$. We give the number of paths in the order $\pi_0, \pi_1, \ldots$.

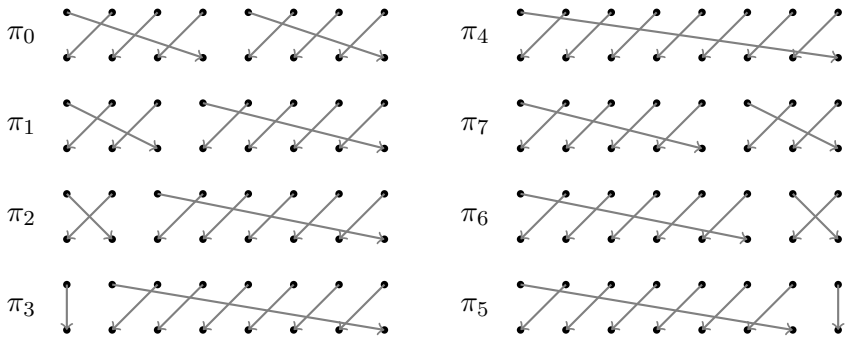
		k				
		2	3	4	5	6
c	0	2,2	1,2	2,5,3	1,2,4	2,5,13,8
	1	-	4,5,5	8,11,15,11	4,12,12,12	8,27,35,44,33
	2	-	-	-	16,23,37,37,23	32,47,83,100,83,47

From this table we see that in all cases where we have carried out direct computation where $c > 0$ we have can find some π_i and π_j such that $\pi_i \neq \pi_j$ but the number of paths from π_i to e is equal to the number of paths from π_j to e. This problem cannot

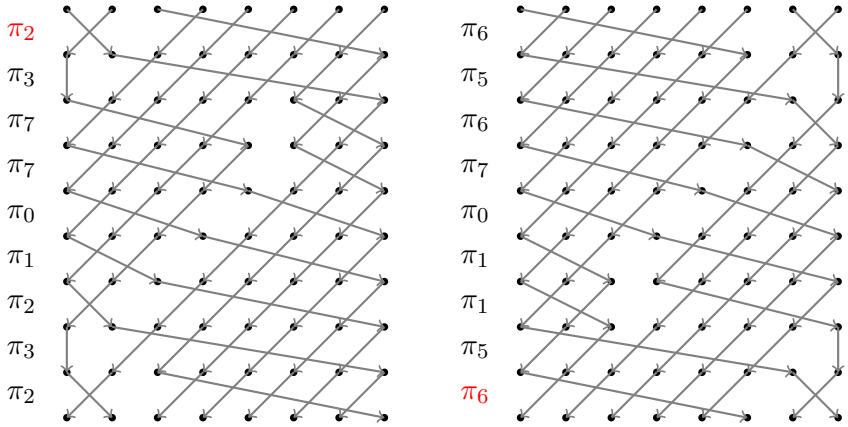
be resolved to allow us to apply the same methods we used to address the case where $c = 0$.

In addition, this table highlights the interesting case of $c = \lceil 1 \rceil + 1$. In this case, we see that the number of closed paths of length $k + 1$ starting with each π_i is equal to the number of closed paths of length $k + 1$ starting with each π_{n-i}. We shall provide an informal proof to show that this difficulty cannot be overcome to make any path counting argument work in this case.

Consider the special case of $k = 8$ and $c = 3$. In this case, we have the rules $\pi_0, \pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6$ and π_7 as follows.



Now consider the closed path $\pi_2\pi_3\pi_7\pi_7\pi_0\pi_1\pi_2\pi_3\pi_2$ and note that if we rotate this path by 180 degrees and reverse the arrows we get another closed path.



Like this from the closed path $\pi_2\pi_3\pi_7\pi_7\pi_0\pi_1\pi_2\pi_3\pi_2$ we can derive the closed path $\pi_6\pi_5\pi_6\pi_7\pi_0\pi_1\pi_1\pi_5\pi_6$.

As indicated by this example, we have that closed paths of a given length beginning with π_2 are in bijective correspondence with closed paths of the same length beginning with π_6, so we cannot consider paths of any length to rule out automorphisms mapping π_2 to π_6 or more generally mapping π_i to π_{k-1}.

Chapter 5

Background to Regular Maps

5.1 Definition

In the second half of our work we shall consider problems in the study of regular maps. The study of regular maps was first formalised by Jones and Singerman in [33] and later by Bryant and Singerman in [9]. We shall begin here by defining regular maps.

First we need to define a *surface*. In our context, a surface will be a connected Hausdorff topological space in which every point has an open neighbourhood homeomorphic to the unit open disc.

We now define an *embedding* of a graph into a surface. The graphs we consider will be restricted to connected undirected graphs containing no semi-edges but possibly containing loops and multi-edges. An *embedding* of a graph G on a surface S shall mean a function ϑ with the following properties. The domain of ϑ shall be contained in $\mathrm{V}(G) \times \mathrm{V}(G) \times \mathrm{E}(G) \times [0,1]$ and the image of ϑ shall be contained in S. We require the following properties.

i) For $u, v \in \mathrm{V}(G)$ and any $u' \sim v' \in \mathrm{E}(G)$ such that $\{u, v\} \neq \{u', v'\}$ we have that $\vartheta(u, v, u' \sim v', r)$ is not defined for any $r \in [0,1]$.

ii) For $u, v \in \mathrm{V}(G)$ and $u \sim v \in \mathrm{E}(G)$ we have $\vartheta(u, v, u \sim v, r) = \vartheta(v, u, u \sim v, 1-r)$ for all $r \in [0,1]$.

iii) For all $u \in \mathrm{V}(G)$ there is some $s_u \in S$ such that for any $v \in \mathrm{V}(G)$ such that $u \sim v$ we have $\vartheta(u, v, u \sim v, 0) = \vartheta(v, u, u \sim v, 1) = s_u$. We shall call s_u the *embedding* of the vertex u in S.

iv) For $u, v \in \mathrm{V}(G)$ the map $\vartheta(u, v, u \sim v, r)$ is continuous for $r \in [0,1]$.

v) For $u, v, u', v' \in \mathrm{V}(G)$, $u \sim v, u' \sim v' \in \mathrm{E}(G)$ and $r, r' \in (0,1)$ we have $\vartheta(u, v, u \sim v, r) = \vartheta(u', v', u' \sim v', r')$ if, and only if, $u \sim v = u' \sim v'$ and either $u = u'$, $v = v'$ and $r = r'$ or $u = v'$, $v = u'$ and $r = 1 - r'$. Informally this means that the images of edges of G do not cross over.

vi) Each connected component of $S \setminus \mathrm{Im}(\vartheta)$ is homeomorphic to the unit open disc.

We may now define a *map* M as a surface S, which we call the *supporting surface* of M; a graph G, which we call the *underlying graph* of M; and an embedding ϑ which satisfies the above rules, which we shall call the *embedding of* G in S. We shall call each of the connected components of $S \setminus \mathrm{Im}(\vartheta)$ the *faces* of the map.

Now that we have defined the notion of a map we shall define symmetries of maps in order to allow us to define regular maps. Informally, we think of a symmetry of a map as being some form of automorphism from the map to itself which preserves the key structure of the map. Hence, in order to define regular maps we now define the *barycentric* subdivision of a map.

For a given map M with supporting surface S, graph G and embedding ϑ, we define a new map M^b as follows. The map M^b shall be defined on the same supporting surface S, but for a different graph G^b and embedding function ϑ^b. First, for each edge $u \sim v = e \in \mathrm{E}(G)$ we introduce a new vertex w_e and replace the edge e in G with the two edges $u \sim w_e$ and $w_e \sim v$ in G^b. We also alter ϑ^b so that $\vartheta^b(w_e, u, w_e \sim u, 0) = \vartheta(u, v, u \sim v, 1/2)$, i.e. we embed w_e half way along the previous edge $u \sim v$, and we define $\vartheta^b(u, w_e, u \sim w_e, r) = \vartheta(u, v, u \sim v, r/2)$ and $\vartheta^b(w_e, v, w_e \sim v, r) = \vartheta(u, v, u \sim v, r/2 + 1/2)$ for $r \in [0, 1]$. Next, for every face of M we introduce a vertex w_f which we embed at an arbitrary point in the face. For every vertex u and edge e of G incident to the face we connect the vertex u and vertex w_e to w_f via an arbitrary line satisfying the above properties. This defines the map M^b. We shall refer to each of the faces of the map M^b, which is made from a mutually incident vertex, edge, face triple of M, as a *flag* of M. Further, we choose to not consider the case of regular maps for which there may be two flags corresponding to the same face, edge, vertex triple (which occurs when the same face is incident to both sides of the same edge). For simplicity we consider these cases degenerate. We shall denote the set of all flags of M as $\mathcal{F}(M)$ and simply refer to it as the *flag set* of M.

We now define the notions of adjacencies of flags. As mentioned previously, flags of M are in bijective correspondence with mutually incident vertex, edge, face triples of M. Hence, we may denote a flag as $\langle v, e, f \rangle$ where v, e and f are a vertex, edge and face respectively which are mutually incident. For two flags $a = \langle v_a, e_a, f_a \rangle$ and $b = \langle v_b, e_b, f_b \rangle$ we shall say the following.

i) a and b are *adjacent along an edge* if $e_a = e_b$ and $f_a = f_b$ but $v_a \neq v_b$;

ii) a and b are *adjacent through a corner* if $v_a = v_b$ and $f_a = f_b$ but $e_a \neq e_b$;

iii) a and b are *adjacent across an edge* if $v_a = v_b$ and $e_a = e_b$ but $f_a \neq f_b$.

We notice that an arbitrary flag f of M is adjacent to exactly one other flag for each of the possible adjacencies. We are now in a position to define automorphisms of a map M. An automorphism of a map M is any function $\phi : \mathcal{F}(M) \to \mathcal{F}(M)$ such that for all $f, f' \in \mathcal{F}(M)$ any adjacencies of f and f' in M are the same as those of $\phi(f)$ and $\phi(f')$ in M. Further, we require that ϕ is a bijection.

We now make the observation that any automorphism ϕ of a map M on a connected surface S with a finite flag set $\mathcal{F}(M)$ is uniquely defined by its action on a single flag of $f \in \mathcal{F}(M)$. This follows from the fact that for a flag f, there are unique flags f_0, f_1 and f_2 adjacent to f along an edge, through a corner and across an edge, and hence if $\phi(f) = f'$ the fact ϕ preserves these adjacencies respectively uniquely determines $\phi(f_0), \phi(f_1)$ and $\phi(f_2)$. Now applying this same argument with f_0, f_1 and f_2 in place of f and noting that M is connected and has only finitely many flags we get the result.

Hence we may now define a regular map. Informally, we want a regular map to be a map with the highest degree of symmetry possible. In order to avoid trivial symmetries, we shall require that a regular map is supported on a connected surface. With this restriction, and the previous observation, we see that the highest degree of symmetry possible is that the automorphism group of a regular map acts transitively on its flag set. Hence we define a regular map as a map whose group of automorphisms acts transitively on its flag set. We note that as the automorphisms of a map are uniquely determined by their action on a single flag in its flag set, we have that the automorphisms of a regular map are in bijective correspondence with its flags.

Now let M be a regular map with flag set $\mathcal{F}(M)$. Let $f \in \mathcal{F}(M)$ and let $x, y, z \in \mathrm{Aut}(M)$ be the automorphisms of M which map f to its neighbours adjacent along an edge, through a corner and across an edge respectively. We note that this means that x, y and z are involutions. We now argue that we must have $\langle x, y, z\rangle = \mathrm{Aut}(M)$. To show this, we must show for any flag $f' \in \mathcal{F}(M)$ the automorphism of M which maps f' to f is in $\langle x, y, z\rangle$. Letting $f' \in \mathcal{F}(M)$ be an arbitrary flag of M, let k be the smallest number such that there is a sequence of flags $f = f_0, f_1, f_2, \ldots, f_k = f'$ such that each f_i and f_{i+1} are adjacent. The existence of said k is clear from connectivity of the supporting surface and finiteness of the flag set. We now prove that the automorphism mapping f' to f is in $\langle x, y, z\rangle$ for each k by induction. For $k \leq 1$ the result is immediate. Now, for $k = c + 1$ with the result for $k = c$, let $h \in \mathrm{Aut}(M)$ be the automorphism of M mapping f' to f, and let $g \in \mathrm{Aut}(M)$ be the automorphism of M mapping f_c to f. By the inductive hypothesis we have $g \in \langle x, y, z\rangle$. As f' is adjacent to f_c we must have that $g^{-1}(f')$ is adjacent to $g^{-1}(f_c) = f$, hence for some $r \in \{x, y, z\}$ we have $r(g^{-1}(f')) = f$ and so $h^{-1} = g^{-1} \circ r \in \langle x, y, z\rangle$.

Hence we have now shown the first important fact about regular maps. Letting M be a regular map, we have that there are $x, y, z \in \mathrm{Aut}(M)$ such that

$$\mathrm{Aut}(M) = \langle x, y, z | x^2 = y^2 = z^2 = (xy)^2 = (yz)^k = (zx)^l = \cdots = e \rangle.$$

We shall refer to the integer k as the *face length* or *face order* and the integer l as the *vertex degree* or *vertex order*.

Conversely, for a given group G with group presentation of the form

$$G = \langle x, y, z | x^2 = y^2 = z^2 = (xy)^2 = (yz)^k = (zx)^l = \cdots = e \rangle,$$

we can also construct a regular map M with flags corresponding to each of the group members of G. The adjacencies of the flags of M may be inferred as follows: the flag corresponding to x is adjacent to e across an edge; the flag corresponding to y is adjacent to e through a corner and the flag corresponding to z is adjacent to e through an edge. Then, in general, the flag corresponding to group member g is adjacent to h across an edge if $h = g^{-1}xg$. Corresponding rules exist for the remaining two types of adjacency. It can be shown that this definition allows a regular map to be uniquely defined corresponding to a group G with identified members x, y and z, and that further the corresponding map M satisfies $\mathrm{Aut}(M) \cong G$. Hence, the study of regular maps can be pursued by studying groups with presentation of the above form.

5.2 Regular Maps by Type

In this section we shall provide a simple, but key result about regular maps. We shall also provide a simple partition of regular maps into three types, in which we may classify all regular maps of the first two types and hence we shall concern ourselves with the study of regular maps of only the third.

Letting M be a regular map on a supporting surface S, the Euler characteristic formula tells us that if S is divided into faces by any graph G as we have described (regular or not), then there is some number χ_S such that $f - e + v = \chi_S$, where f is the number of faces M is divided into by G, e is the number of edges of G and v is the number of vertices of G. This number χ_S is invariant for S and independent of the choice of graph G, and is called the *Euler characteristic* of S.

Now, for a given regular map M with automorphism group $\mathrm{Aut}(M) = \langle x, y, z \rangle$ where x is an involution along an edge, y is an involution across an edge and z is an involution through a corner, we can calculate the numbers f, e and v as follows. Each

face in a regular map contains the same number of flags from the flag set, and if k is the face length of M then the number of flags per face is $2k$. The total number of flags in the regular map is equal to the size of the automorphism group of M, so the number of faces in the regular map is given by $|G|/2k$. Further, we can find k as the order of the element yz in $\mathrm{Aut}(M)$, hence $f = |G|/2k = |G|/2|\langle yz\rangle|$. By similar reasoning we find that the number of edges in M is $e = |G|/4 = |G|/2|\langle xy\rangle|$ and the number of vertices in M is $v = |G|/2l = |G|/2|\langle zx\rangle|$. Hence, for a given surface S we have the following formula

$$|G|/2k - |G|/4 + |G|/2l = \chi_S.$$

Rearranging, we get

$$|G|(1/k - 1/2 + 1/l)/2 = \chi_S \quad \Leftrightarrow \quad |G| = 2\chi_S/(1/k - 1/2 + 1/l).$$

We shall consider the following three cases.

i) $1/k + 1/l > 1/2$,

ii) $1/k + 1/l = 1/2$,

iii) $1/k + 1/l < 1/2$.

Regular maps in case (i) are called *spherical*. For $k, l \geq 3$ the only solutions for $1/k + 1/l > 1/2$ are $(k, l) \in \{(3,3), (3,4), (3,5), (4,3), (5,3)\}$. In this case from $|G| = 2\chi_S/(1/k - 1/2 + 1/l)$ we must have that $\chi_S > 0$, and as $\chi_S \leq 2$ is an integer this gives us $\chi_S = 2$ or $\chi_S = 1$. The only surfaces with $\chi_S = 2$ or $\chi_S = 1$ are the sphere and the projective plane respectively. In each of these cases we may find the size of the group G and classify all possible regular maps with these parameters. For the remaining cases where at least one of k or l is 2 there are four readily classifiable infinite classes of regular map on the sphere and on the projective plane.

Regular maps in case (ii) are called *Euclidean*. These maps satisfy $1/k - 1/2 + 1/l = 0$ and hence are supported on surfaces S for which $\chi_S = 0$. The surfaces S where $\chi_S = 0$ are the Euclidean plane, the torus and the Klein bottle. The parameters k and l for which $1/k + 1/l = 2$ are $(k, l) \in \{(3,6), (4,4), (6,3)\}$. The regular maps in this category on the Euclidean plane are regular tilings by hexagons, squares and triangles, and the regular maps in this category on the torus are quotients of the regular maps on the whole plane, and are readily classifiable. Further, there are no regular maps on the Klein bottle, we refer to [17] and [49] for proofs of this fact.

Finally, the regular maps in case (iii) are called *hyperbolic*. This forms the most interesting case of regular maps and shall be the primary focus of our attention. In this case we have $1/k - 1/2 + 1/l = -\alpha$ for some rational $\alpha > 0$. We have $\chi_S = -\alpha|G|/2 < 0$, hence all hyperbolic regular maps are supported on surfaces with negative Euler characteristic. Further, for a given surface S of negative Euler characteristic we also see any regular map supported on S must be hyperbolic. From the expression $|G| = -2\chi_S/(1/2 - 1/k - 1/l)$ we see that $|G|$ is at a maximum when $1/2 - 1/k - 1/l$ is at a minimum. Trivial analysis will show that $1/2 - 1/k - 1/l$ is at a minimum for $(k, l) = (3, 7)$ or $(7, 3)$, giving $1/2 - 1/k - 1/l = 1/42$, and so $|G| = -84\chi_S$. Altogether this shows that for a given surface S of negative Euler characteristic χ_S there are at most finitely many regular maps supported on S corresponding to groups of size no greater than $-84\chi_S$.

From this initial argument we find a potential classification strategy for regular maps in which regular maps are classified by the Euler characteristic of their supporting surfaces. Indeed, this has been done in the spherical and Euclidean cases and in the hyperbolic case for each Euler characteristic there are only finitely many regular maps. To this end, all regular maps for given small negative Euler characteristic have been classified by Conder in the online lists [14] and [13]. Further, other efforts have been made to understand, characterise and classify regular maps for certain special negative Euler characteristic, such as the classification of regular maps on negative prime Euler characteristic by D'Azevedo, Nedela and Širáň in [19].

5.3 External Symmetries

We have seen that a regular map is a map possessing as large a possible automorphism group for a given size of flag set. However, it is also possible for a regular map to possess further external symmetries, which are automorphisms of the automorphism group itself. We shall now define two dual operators on regular maps from which we may define two external symmetries of regular maps which we will be particularly interested in.

First, we define the *dual* of a regular map. Informally, the dual of a regular map is formed by interchanging the role of the vertices and faces of a regular map. Formally, in our definition of a regular map M with barycentric subdivision M^b, this interchange of roles is equivalent to exchanging the roles of the vertices w_v and w_f, we may then obtain a new regular map N, the dual of M, denoted $\mathrm{D}(M)$, by taking each w_f to be the vertices of N, and the paths $w_f \sim w_e \sim w_{f'}$ to be the edges in N. We note from this method of construction it is trivial that M and its dual share the same

flag set, and thus the same automorphism group.

Now suppose that M and N are a regular map and its dual both on the same flag set $\mathcal{F}(M)$. For each of M and N fix some flag $f \in \mathcal{F}(M)$ and denote by x_M, y_M and z_M the automorphisms of M gained by mapping f to a flag adjacent along an edge, through a corner and across an edge of M respectively; and x_N, y_N and z_N to be automorphsims of N mapping f to a flag adjacent along an edge, through a corner and across an edge of N respectively. As we have shown before, this gives us

$$\mathrm{Aut}(M) = \langle x_M, y_M, z_M \rangle \quad \text{and} \quad \mathrm{Aut}(N) = \langle x_N, y_N, z_N \rangle.$$

From the construction of the dual of a regular map we have the further property that there is a unique isomorphism $\phi : \mathrm{Aut}(M) \to \mathrm{Aut}(N)$ satisfying $\phi(x_M) = y_N$, $\phi(y_M) = x_N$, $\phi(z_M) = z_N$ and $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in M$. Hence we may think of the dual of a regular map M in terms of interchanging the roles of x and y in its automorphism group.

We will now further call a map *self dual* if it is isomorphic to its dual. We note that this isomorphism implies that the function ϕ described above satisfies that $\phi : \mathrm{Aut}(M) \to \mathrm{Aut}(M)$ and ϕ is non-trivial. We shall call any $\psi \in \mathrm{Aut}(\mathrm{Aut}(M))$ an *external automorphism* of M, and hence the property of being self dual can be seen as having a particular non-trivial external symmetry of the automorphism group.

The second operator we will be interested in will be the Petrie dual of a regular map. The definition of the Petrie dual is more involved than what we have encountered thus far, and so we shall satisfy ourselves with an informal description of the Petrie dual and an equivalent formal description of the automorphism of the group of the regular map.

For a regular map M on supporting surface S we can create the Petrie dual of M as follows. Consider an arbitrary vertex v and edge e of M such that v is incident to v, and pick a face f such that f is incident to e. We describe a path along the surface S of M. We start this path from a point on f close to v and move in the direction of e close to e. When we approach the midpoint of e, we turn and cross over the edge e onto the face f' of M adjacent to f through e. We then continue the path in the same direction along e approaching the vertex v' of M which is connected to v by the edge e. The path is continued along e until we get close to v'. We now continue creating the path in the same way, but this time with respect to the vertex v', face f' and the edge e' which is the only edge of M adjacent to f' and v' other than e. Eventually, this path will arrive back at v, where we connect to the start to form a loop. This

path is called the *Petrie dual walk* or *Petrie walk* of M, which is unique to isomorphism due to the regularity of M. We shall call the number of edges crossed in the path the *Petrie dual walk length* of M, or the *Petrie dual order*.

We continue creating the Petrie dual of M by considering the all Petrie walks of M starting from each mutually incident face, vertex, edge triple. For each Petrie walk we consider "cutting" along the walk and creating a new face along the walk. Further, at each crossing point in the centre of an edge rather than have the two Petrie walks along either side of the edge meet we instead add a twist so that the two paths form a half helix with one another. The new shape that we create is then itself a regular map. We shall call this regular map the *Petrie dual* of M, denoted $\mathrm{P}(M)$.

Equivalent to our given definition of the Petrie dual is the characterisation of the Petrie dual as an external symmetry of a map M. Let M be an arbitrary regular map, and let $N = \mathrm{P}(M)$ be its Petrie dual. Let x, y and z be the involutions gained by mapping some arbitrary fixed flag f to a flag adjacent along an edge, through a corner and across an edge respectively, as before, such that $\mathrm{Aut}(M) = \langle x_M, y_M, z_M \rangle$ and $\mathrm{Aut}(N) = \langle x_N, y_N, z_N \rangle$. We now have that the function $\phi : \mathrm{Aut}(M) \to \mathrm{Aut}(N)$ given by $\phi(x_M) = x_N y_N$, $\phi(y_M) = y_N$, $\phi(z_M) = z_N$ and $\phi(gh) = \phi(g)\phi(h)$ is an isomorphism from $\mathrm{Aut}(M)$ to $\mathrm{Aut}(N)$. In the case that N is isomorphic to M we call M *self Petrie dual*, and in this case we see that ϕ is an automorphism of the automorphism group of the regular map M, i.e. an external symmetry.

In light of this view of automorphism group in terms of the Petrie dual we shall expand our notation of a (k, l)-regular map where k is the face length and l the vertex degree to (k, l, m)-regular maps where k and l are as before and m is the Petrie dual walk length. In this case, we will call k, l and m the face, vertex and Petrie orders to be concise. Now, recall that a (k, l)-regular map M has a group presentation of the form

$$\langle x, y, z | x^2 = y^2 = z^2 = (xy)^2 = (yz)^k = (zx)^l = \cdots = e \rangle.$$

Now we note from the previous that the face length of the Petrie dual $\mathrm{P}(M)$ of M is the order of the element zxy. Further, the face order of $\mathrm{P}(M)$ is the Petrie order of M. Hence, a (k, l, m)-regular map has a group presentation of the form

$$\langle x, y, z | x^2 = y^2 = z^2 = (xy)^2 = (yz)^k = (zx)^l = (zxy)^m = \cdots = e \rangle.$$

5.4 Problems

The research into regular maps covers many different sub areas focusing on particular problems of interest. Most notably for our purposes are the existence problems and the classification problems. We have already seen that classification of regular maps on given supporting surfaces is one approach to classification of regular maps.

In our work we shall consider two problems in regular maps as follows.

i) For every triple $k, l, m \in \mathbb{N}$ such that each pair is hyperbolic does there exist a finite (k, l, m)-regular map?

ii) For which $k \in \mathbb{N}$ do there exist finite regular maps of degree k which are both self dual and self Petrie dual?

Problem (i) represents a new direction of research in considering regular maps. The problem was originally proposed by Širáň at the *Symmetries of Surfaces, Maps and Dessins* workshop in Banff, September 2017 (for which no written record exists). We shall provide some initial results towards answering this question. The method by which we shall address this question will be to construct regular maps for given (k, l, m) triples. The question of when there exist (k, l, m)-regular maps is related to the study of groups of a particular form first studied by Coxeter. The (k, l, m)-regular maps are exactly the smooth quotients of these groups. Further to this question one may consider the possible classification of all (k, l, m)-regular maps for a given triple (k, l, m). We shall comment on the connection between our work and this question, and the relationship to the groups of Coxeter.

Problem (ii) is already solved in the case that k is even by an explicit construction of a self dual and self Petrie dual regular map. The proof is available in the Final Report of the *Symmetries of Surfaces, Maps and Dessins* workshop in Banff [15]. We shall approach the case that k is odd with an unrelated construction of self dual and self Petrie dual regular maps for all k except for a finitely computable set of exceptional cases.

Chapter 6

Regular Maps of Given Face, Vertex and Petrie Orders

6.1 Introduction

In this chapter we shall study the question of for which triples $k, l, m \in \mathbb{N}$ there exist (k, l, m)-regular maps. We shall focus on the case of each pair of k, l, m being hyperbolic. We shall attempt a direct construction of a (k, l, m)-regular map for a given triple, following the construction of Wilson in [51], and the approach of Jones, Mačaj and Širáň in [34]. The approach we take is as follows.

i) From the classification of regular maps in fractional linear groups which may be taken from [16] we extract generator matrices for regular maps with given face and vertex orders;

ii) The Petrie dual order of the above maps may then be derived. Specifying the Petrie dual order of these maps can then be expressed as a further condition;

iii) We then express the simultaneous conditions of finding a regular map with a given face, vertex and Petrie order as being equivalent to finding a root to a polynomial in an arbitrary finite field of a given order;

iv) Analysis of the final condition will allow us to say exactly when roots of particular orders exist.

The work necessary to derive these conditions and analyse the related problem in finite fields is lengthy and abstract. Further, it is the result of generalising more intuitive arguments which solve sub problems of the original problem. Hence, we shall present the approach in a chronological order including results and methods later superseded. We choose this approach for a more clear and transparently motivated exposition.

6.2 Regular Maps in Fractional Linear Groups

We begin our construction of hyperbolic (k, l, m)-regular maps for given triples $k, l, m \in \mathbb{N}$ by deriving conditions on when such maps exist in fractional linear groups.

6.2.1 Summary of Regular Maps in Fractional Linear Groups

First, we summarise the classification of regular maps over fractional linear groups which can be extracted from the paper [16] of Conder, Potočnik and Širáň classifying regular hypermaps over the same groups. In the classification we shall also get explicit forms for generator matrices for these groups which will be especially useful in our work.

In the first half of this section, we assume that p is an odd prime and let K be an algebraically closed field of characteristic p. We first define the following matrices in $\mathrm{SL}(2, K)$ which we shall use throughout. In the following we use ξ_n to denote an n^{th} root of unity, and ω_n to denote an element of the form $\xi_n + \xi_n^{-1}$.

$$X_1 = \eta_1\beta_1 \begin{pmatrix} D_1 & \omega_{2l}\xi_{2k}D_1 \\ -\omega_{2l}\xi_{2k}^{-1} & -D_1 \end{pmatrix}, \quad Y_1 = \beta_1 \begin{pmatrix} 0 & \xi_{2k}D_1 \\ \xi_{2k}^{-1} & 0 \end{pmatrix}, \quad Z_1 = \beta_1 \begin{pmatrix} 0 & D_1 \\ 1 & 0 \end{pmatrix},$$

where $\eta_1 = (\xi_{2k} - \xi_{2k})^{-1}$, $\beta_1 = -1/\sqrt{-D_1}$, $D_1 = \omega_{2k}^2 + \omega_{2l}^2 - 4$.

$$X_2 = \beta_2 \begin{pmatrix} 0 & \omega_{2l}^2 \\ 1 & 0 \end{pmatrix}, \quad Y_2 = \eta_2\beta_2 \begin{pmatrix} \omega_{2l}^2 & 2\omega_{2l}^2 \\ -2 & -\omega_{2l}^2 \end{pmatrix}, \quad Z_2 = \beta_2 \begin{pmatrix} 0 & \xi_{2l}\omega_{2l}^2 \\ \xi_{2l}^{-1} & 0 \end{pmatrix},$$

where $\eta_2 = (\xi_{2l} - \xi_{2l}^{-1})^{-1}$, $\beta_2 = -1/\sqrt{-D_2}$ $D_2 = \omega_{2l}^2$.

$$X_3 = \alpha \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \quad Y_3 = \alpha \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad Z_3 = \alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

where $\alpha^2 = -1$.

Further, we define the groups $G_n \leq \mathrm{SL}(2, K)$ and their projections $\overline{G}_n \leq \mathrm{PSL}(2, K)$ as follows.

$$G_1(\xi_{2k}, \xi_{2l}) = \langle X_1, Y_1, Z_1 \rangle, \qquad \overline{G}_1(\xi_{2k}, \xi_{2l}) = \langle \overline{X}_1, \overline{Y}_1, \overline{Z}_1 \rangle,$$
$$G_2(\xi_{2l}) = \langle X_2, Y_2, Z_2 \rangle, \qquad \overline{G}_2(\xi_{2l}) = \langle \overline{X}_2, \overline{Y}_2, \overline{Z}_2 \rangle,$$
$$G_3 = \langle X_3, Y_3, Z_3 \rangle, \qquad \overline{G}_3 = \langle \overline{X}_3, \overline{Y}_3, \overline{Z}_3 \rangle.$$

Likewise, the regular map generated by $\overline{X}_1, \overline{Y}_1, \overline{Z}_1 \in \overline{G}_1(\xi_{2k}, \xi_{2l})$ shall be called $M_1(\xi_{2k}, \xi_{2l})$ etc. We note that in each case we have $M = \langle \overline{X}, \overline{Y}, \overline{Z} \rangle$ where $\mathrm{ord}(\overline{X}) = \mathrm{ord}(\overline{Y}) = \mathrm{ord}(\overline{Z}) = 2$, $\mathrm{ord}(\overline{XY}) \in \{k, p\}$ and $\mathrm{ord}(\overline{YZ}) \in \{l, p\}$. We now state the key results we shall use.

Theorem 6.1 (Conder, Potočnik, Širáň)**.** *A hyperbolic (k,l)-regular map M has automorphism group a fractional linear group over a field of characteristic p if, and only if, one of the following cases occurs*

Case (i) $p \nmid k, l$ and there are some ξ_{2k}, ξ_{2l} such that $D_1 \neq 0$ and $M \cong M_1(\xi_{2k}, \xi_{2l})$;

Case (ii) $k = p \nmid l$ and there is some ξ_{2l} such that $D_2 \neq 0$ and $M \cong M_2(\xi_{2l})$;

Case (iii) $k = l = p$ and $M \cong M_3$.

We now give the corresponding theorem for the case of $p = 2$. As no hyperbolic pairs k, l have $k = 2$ or $l = 2$, we only have to consider one case when $p = 2$. We define the following matrices.

$$X_4 = \eta_4\beta_4 \begin{pmatrix} D_4 & \omega_l\xi_k D_4 \\ \omega_l\xi_k^{-1} & D_4 \end{pmatrix}, \quad Y_4 = \beta_4 \begin{pmatrix} 0 & \xi_k D_4 \\ \xi_k^{-1} & 0 \end{pmatrix}, \quad Z_4 = \beta_4 \begin{pmatrix} 0 & D_4 \\ 1 & 0 \end{pmatrix},$$

$$\text{where} \quad \eta_4 = (\xi_k + \xi_k^{-1})^{-1}, \qquad \beta_4 = 1/\sqrt{D_4}, \qquad D_4 = \omega_k^2 + \omega_l^2.$$

Further we define the corresponding $G_4(\xi_k, \xi_l)$ and $M_4(\xi_k, \xi_l)$. In this case we have $\mathrm{PSL}(2, K) \cong \mathrm{SL}(2, K)$, hence do not define $\overline{G}_4$. We now have the corresponding theorem.

Theorem 6.2 (Conder, Potočnik, Širáň)**.** *A hyperbolic (k,l)-regular map M has automorphism group a fractional linear group of character 2 if, and only if, $2 \nmid k, l$ and there exist some ξ_k, ξ_l such that $D_4(\xi_k, \xi_l) \neq 0$ and $M \cong M_4(\xi_k, \xi_l)$.*

6.2.2 Equivalent Conditions

In this section we shall derive equivalent conditions for the existence of (k,l,m)-regular maps in fractional linear groups. We shall first begin with some lemmas.

In the following, for any n we shall write ξ_n and ξ_{2n} to denote primitive roots of order n and $2n$ respectively which satisfy the relationship $\xi_n = \xi_{2n}^2$. If we fix ξ_{2n} then we

may simply take $\xi_n = \xi_{2n}^2$ and we are done. However, if instead we fix some ξ_n we must show that an appropriate choice of ξ_{2n} exists satisfying the relationship.

Lemma 6.3. *For any n, if ξ_n is a primitive root of order n there exists a ξ_{2n} such that $\xi_{2n}^2 = \xi_n$.*

Proof. Let $\alpha, -\alpha$ be the solutions of $x^2 = \xi_n$ in K. From $\alpha^{2n} = \xi_n^n = 1$ we have $\mathrm{ord}(\alpha) \mid 2n$. If $\mathrm{ord}(\alpha) = m$ then we have $1 = \alpha^{2m} = \xi_n^m$, so we have $n \mid \mathrm{ord}(\alpha) \mid 2n$, and $\mathrm{ord}(\alpha)$ is either n or $2n$. We now consider the two cases of whether $\mathrm{ord}(\alpha)$ is even or odd. If $\mathrm{ord}(\alpha) = 2m$ for some m is even, then $1 = \alpha^{2m} = \xi_n^m$ and so $m = n$ and we may take $\xi_{2n} = \alpha$. If $\mathrm{ord}(\alpha) = m$ is odd then $\mathrm{ord}(-\alpha) = 2m$ is even and we may take $\xi_{2n} = -\alpha$. □

We note that in our notation we shall require for given n that ξ_n and ξ_{2n} satisfy the relationship $\xi_n = \xi_{2n}^2$. In particular, this relationship is only required when the subscripts are both expressed in terms of n. If there is some other subscript k not expressed in terms of n such that we happen to have $k = 2n$ we do not require $\xi_n = \xi_k^2$. In the following we let $\Phi_n(x) \in \mathbb{Z}[x]$ denote the n^{th} cyclotomic polynomial, and $\Psi_n(x) \in \mathbb{Z}[x]$ denote the unique polynomial satisfying $x^{\varphi(n)/2}\Psi_n(x + x^{-1}) = \Phi_n(x)$.

Lemma 6.4. *In K we have $\omega_p = 2$ and $\omega_{2p} = -2$.*

Proof. In our notation ω_n is defined to be a root of $\Psi_n(x)$. Hence we shall show that $\Psi_p(x) = (x-2)^{(p-1)/2}$ and $\Psi_{2p}(x) = (x+2)^{(p-1)/2}$ in K. This is a consequence of the fact that $\Phi_p(x) = (x-1)^{p-1}$ and $\Phi_{2p}(x) = (x+1)^{p-1}$ in K, and the identity $x^{\varphi(n)/2}\Psi_n(x + x^{-1}) = \Phi_n(x)$. Letting $f(x) = (x-2)^{(p-1)/2}$ and $g(x) = (x+2)^{(p-1)/2}$ we have

$$\begin{aligned} x^{\varphi(p)/2} f(x + x^{-1}) &= x^{(p-1)/2}(x + x^{-1} - 2)^{(p-1)/2} \\ &= (x^2 - 2x + 1)^{(p-1)/2} = (x-1)^{p-1} = \Phi_p(x), \end{aligned}$$

and

$$\begin{aligned} x^{\varphi(2p)/2} g(x + x^{-1}) &= x^{(p-1)/2}(x + x^{-1} + 2)^{(p-1)/2} \\ &= (x^2 + 2x + 1)^{(p-1)/2} = (x+1)^{p-1} = \Phi_{2p}(x). \end{aligned}$$

Therefore $\Psi_p(x) = f(x)$ and $\Psi_{2p}(x) = g(x)$. □

In the following we make use of the facts that if $X \in \mathrm{SL}(2, K)$ then $\mathrm{ord}(X) = n$ if, and only if, $\mathrm{tr}(X) = \omega_{2n}$ for some $\omega_{2n} \in K$; and if $\mathrm{ord}(X) = 2n$ is even then $\mathrm{ord}(\overline{X}) = n$.

Lemma 6.5. *For any $\overline{X} \in \mathrm{PSL}(2,K)$ with pre-image $X \in \mathrm{SL}(2,K)$, we have $\mathrm{ord}(\overline{X}) = n$ if, and only if, $\mathrm{tr}(X)^2 = \omega_{2n}^2$ for some element $\omega_{2n} \in K$.*

Proof. We shall consider the cases $p \mid n$ and $p \nmid n$ separately. For $p \nmid n$, first suppose that $\mathrm{ord}(\overline{X}) = n$ and X is a pre-image of $\overline{X}$. As X is a pre-image of $\overline{X}$ we have either $\mathrm{ord}(X) = n$ and n is odd or $\mathrm{ord}(X) = 2n$. If $\mathrm{ord}(X) = 2n$ then $\mathrm{tr}(X) = \omega_{2n}$ and we are done. If $\mathrm{ord}(X) = n$ then $\mathrm{tr}(X)^2 = \mathrm{tr}(-X)^2 = \omega_{2n}^2$ and we are done. Conversely, if $\mathrm{tr}(X)^2 = \omega_{2n}^2$ then, without loss of generality, we may take $\mathrm{tr}(X) = \omega_{2n}$ and $\mathrm{tr}(-X) = -\omega_{2n}$, giving $\mathrm{ord}(X) = 2n$ and so $\mathrm{ord}(\overline{X}) = n$.

For $p \mid n$ suppose that X is a pre-image of $\overline{X}$. As X is a pre-image of $\overline{X}$ we have either $\mathrm{ord}(X) = p$ or $\mathrm{ord}(X) = 2p$. In the first case we have $\mathrm{tr}(X) = 2$ and in the second case we have $\mathrm{tr}(X) = -2$. Hence, in either case we have $\mathrm{tr}(X)^2 = 4 = \omega_{2p}^2$. Conversely, if $\mathrm{tr}(X)^2 = \omega_{2p}^2 = 4$ when $\mathrm{tr}(X) = 2$ or $\mathrm{tr}(X) = -2$, giving $\mathrm{ord}(X) = p$ or $\mathrm{ord}(X) = 2p$ respectively. In either case, $\mathrm{ord}(\overline{X}) = p$. □

Lemma 6.6. *For any finite field K of characteristic p and fixed $\omega_k, \omega_l \in K$ there is a uniquely determined element $\omega = \xi + \xi^{-1}$ such that $\omega_k + \omega_l + \omega + 2 = 0$. Further, we can uniquely define a number m either by $m = \mathrm{ord}(\xi) = \mathrm{ord}(\xi^{-1})$ or, if $\xi = \xi^{-1} = 1$, by $m = p$. In either case, we have that ω is a root of $\Psi_m(x)$.*

Proof. Clearly ω is uniquely defined from $\omega = -(\omega_k + \omega_l + 2)$. Defining ξ and ξ^{-1} by $\xi + \xi^{-1} = \omega$ we see we may rearrange to get $\xi^2 - \omega\xi + 1 = 0$. Hence, considering the polynomial $f(x) = x^2 - \omega x + 1$ we see that ξ and ξ^{-1} are the uniquely determined roots of $f(x)$ in K.

If $\mathrm{ord}(\xi) \neq 1$ we have that $p \nmid \mathrm{ord}(\xi)$ and, letting $m = \mathrm{ord}(\xi) = \mathrm{ord}(\xi^{-1})$, we have $\Phi_m(\xi) = 0$ and so $\Psi_m(\omega) = \Psi_m(\xi + \xi^{-1}) = \xi^{-\varphi(m)/2}\Phi_m(\xi) = 0$. Therefore in this case we may define $m = \mathrm{ord}(\xi) = \mathrm{ord}(\xi^{-1})$ and we have that ω is a root of Ψ_m.

If $\mathrm{ord}(\xi) = 1$ then we have $\xi = \xi^{-1} = 1$. Hence we have $\omega = 2$ and by Lemma 6.4 we have that $\Psi_p(\omega) = 0$. □

From here onward we will allow ourselves to define ω_m to be the unique solution to the equation $\omega_k + \omega_l + \omega_m + 2 = 0$ for given ω_k and ω_l, noting that this also uniquely defines m, which we take to be p in the special case just outlined.

We now introduce a series of propositions showing the relationship between the maps $M_1(\xi_{2k}, \xi_{2l})$, $M_2(\xi_{2l})$, M_3 and $M_4(\xi_k, \xi_l)$ as defined above and the length of their Petrie dual walks.

Proposition 6.7. *For $\xi_{2k}, \xi_{2l} \in K$ such that $D_1(\xi_{2k}, \xi_{2l}) \neq 0$ the map $M_1(\xi_{2k}, \xi_{2l})$ is a (k, l, m)-regular map where m is given by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. From Theorem 6.1 we know that $M_1(\xi_{2k}, \xi_{2l})$ is a (k, l)-regular map. Therefore, we simply calculate the Petrie order of $M_1(\xi_{2k}, \xi_{2l})$. The Petrie order of $M_1(\xi_{2k}, \xi_{2l})$ is given by the order of the element $\overline{Z}_1\overline{X}_1\overline{Y}_1$ in $\overline{G}_1$. Using Lemma 6.5 we may calculate $m = \mathrm{ord}(\overline{Z}_1\overline{X}_1\overline{Y}_1)$ by calculating $\mathrm{tr}(Z_1X_1Y_1)^2 = \omega_{2m}$. We calculate $Z_1X_1Y_1$ as follows.

$$\begin{aligned} Z_1X_1Y_1 &= \eta_1\beta_1^3 \begin{pmatrix} 0 & D_1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} D_1 & \omega_{2l}\xi_{2l}D_1 \\ \omega_{2l}\xi_{2l}^{-1} & -D_1 \end{pmatrix} \begin{pmatrix} 0 & \xi_{2k}D_1 \\ \xi_{2k}^{-1} & 0 \end{pmatrix} \\ &= -\eta_1\beta_1 \begin{pmatrix} \omega_{2l}\xi_{2l}^{-1} & -D_1 \\ 1 & \omega_{2l}\xi_{2l} \end{pmatrix} \begin{pmatrix} 0 & \xi_{2k}D_1 \\ \xi_{2k}^{-1} & 0 \end{pmatrix} = -\eta_1\beta_1 \begin{pmatrix} -\xi_{2k}^{-1}D_1 & \omega_{2l}D_1 \\ \omega_{2l} & \xi_{2k}D_1 \end{pmatrix}. \end{aligned}$$

Hence we have $\mathrm{tr}(Z_1X_1Y_1) = -\eta_1\beta_1(\xi_{2k} - \xi_{2k}^{-1})D_1 = -D_1/\sqrt{-D_1}$. Therefore we have $\omega_{2m}^2 = -D_1 = 4 - \omega_{2k}^2 - \omega_{2l}^2$, and so $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$. Noting that $\omega_{2n}^2 = (\xi_{2n} + \xi_{2n}^{-1})^2 = \xi_n + \xi_n^{-1} + 2 = \omega_n + 2$ we may rearrange this equation to show $\omega_k + \omega_l + \omega_m + 2 = 0$. By Lemma 6.6, m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$. □

Proposition 6.8. *For $\xi_{2l} \in K$ such that $D_2(\xi_{2l}) \neq 0$ the map $M_2(\xi_{2l})$ is a (k, l, m)-regular map where $k = p$, $\omega_k = \omega_p$ and m is given by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. We proceed as in the previous proposition. We calculate $\omega_{2m}^2 = \mathrm{tr}(Z_2X_2Y_2)^2$ as follows.

$$\begin{aligned} Z_2X_2Y_2 &= \eta_2\beta_2^3 \begin{pmatrix} 0 & \xi_{2l}\omega_{2l}^2 \\ \xi_{2l}^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega_{2l}^2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega_{2l}^2 & 2\omega_{2l}^2 \\ -2 & -\omega_{2l}^2 \end{pmatrix} \\ &= -\eta_2\beta_2 \begin{pmatrix} \xi_{2l} & 0 \\ 0 & \xi_{2l}^{-1} \end{pmatrix} \begin{pmatrix} \omega_{2l}^2 & 2\omega_{2l}^2 \\ -2 & -\omega_{2l}^2 \end{pmatrix} = -\eta_2\beta_2 \begin{pmatrix} \xi_{2l}\omega_{2l}^2 & 2\xi_{2l}\omega_{2l}^2 \\ -2\xi_{2l}^{-1} & -\xi_{2l}^{-1}\omega_{2l}^2 \end{pmatrix}. \end{aligned}$$

This gives $\mathrm{tr}(Z_2X_2Y_2) = -\eta_2\beta_2(\xi_{2l} - \xi_{2l}^{-1})\omega_{2l}^2 = \omega_{2l}^2/\sqrt{-\omega_{2l}^2}$. Hence $\omega_{2m}^2 = \mathrm{tr}(Z_2X_2Y_2)^2 = -\omega_{2l}^2$. This gives $\omega_{2l}^2 + \omega_{2m}^2 = 0$. As $k = p$ we have $\omega_{2k}^2 = 4$, giving $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$, and so as before ω_m is given by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$. □

Proposition 6.9. *The map M_3 is a (k, l, m)-regular map where $k = l = p$, $\omega_k = \omega_l = \omega_p$ and m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. We calculate $\omega_{2m}^2 = \mathrm{tr}(Z_3X_3Y_3)^2$ as follows.

$$\begin{aligned} Z_3X_3Y_3 &= \alpha^3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \\ &= -\alpha \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} = -\alpha \begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}. \end{aligned}$$

This gives $\mathrm{tr}(Z_3X_3Y_3) = -2\alpha$ and hence $\mathrm{tr}(Z_3X_3Y_3)^2 = -4$. Therefore, as $\omega_{2k}^2 = \omega_{2l}^2 = 4$ we have $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$, and so ω_m is given by the unique solution to $\omega_k + \omega_l + \omega_m = 2$ as previously. □

We now deal with the case $p = 2$.

Proposition 6.10. *For $\xi_k, \xi_l \in K$ such that $D_4(\xi_k, \xi_l) \neq 0$ the map $M_4(\xi_k, \xi_l)$ is a (k, l, m)-regular map where m is defined by the unique solution to $\omega_k + \omega_l + \omega_m + 2 = 0$.*

Proof. Lemma 6.5 does not apply in this case. However, for any $2 \nmid n$ we have $\mathrm{ord}(M) = n$ if, and only if, $\mathrm{tr}(M) = \omega_n$ for $M \in \mathrm{SL}(2, K)$. Hence, we take $\omega_m = \mathrm{tr}(Z_4X_4Y_4)$ where m is the Petrie order of $M_4(\xi_k, \xi_l)$. We calculate $Z_4X_4Y_4$ as follows.

$$\begin{aligned} Z_4X_4Y_4 &= \eta_4\beta_4^3 \begin{pmatrix} 0 & D_4 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} D_4 & \omega_l\xi_kD_4 \\ \omega_l\xi_k^{-1} & D_4 \end{pmatrix} \begin{pmatrix} 0 & \xi_kD_4 \\ \xi_k^{-1} & 0 \end{pmatrix} \\ &= \eta_4\beta_4 \begin{pmatrix} \omega_l\xi_k^{-1} & D_4 \\ 1 & \omega_l\xi_k \end{pmatrix} \begin{pmatrix} 0 & \xi_kD_4 \\ \xi_k^{-1} & 0 \end{pmatrix} = \eta_4\beta_4 \begin{pmatrix} \xi_k^{-1}D_4 & \omega_lD_4 \\ \omega_l & \xi_kD_4 \end{pmatrix}. \end{aligned}$$

Hence $\mathrm{tr}(Z_4X_4Y_4) = \eta_4\beta_4(\xi_k + \xi_k^{-1})D_4 = D_4/\sqrt{D_4}$. This gives $\omega_m^2 = D_4 = \omega_k^2 + \omega_l^2$, which is equivalent to $\omega_k^2 + \omega_l^2 + \omega_m^2 = 0$ so, as squaring is the Frobenius automorphism in finite fields of characteristic 2, we have $\omega_k + \omega_l + \omega_m + 2 = 0$ as required. □

We now have the groundwork necessary to prove our first important proposition regarding regular maps in fractional linear groups. The following result is original work of the author.

Proposition 6.11. *There exists a hyperbolic (k, l, m)-regular map in a fractional linear group of characteristic p if, and only if, there is a solution to the equation*

$$\omega_k + \omega_l + \omega_m + 2 = 0$$

in a finite field of characteristic p where, for each $n \in \{k, l, m\}$, either $n = p$ or $p \nmid n$, and we do not have $(k, l, m) = (p, p, p)$.

Proof. The Theorems 6.1 and 6.2 of Conder, Potočnik and Širáň combined with Propositions 6.7, 6.8, 6.9 and 6.10 shows that if M is a hyperbolic (k, l, m)-regular map with automorphism group a fractional linear group over a field of characteristic p then there is a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ in a suitable extension of GF(p).

Now, conversely, suppose that we have a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ for some hyperbolic triple k, l, m in a finite field of characteristic p. If $p \neq 2$, we first define ξ_{2k}, ξ_{2l} and ξ_{2m} using Lemma 6.3. As k, l, m is a hyperbolic triple we have $\omega_{2m}^2 \neq \omega_4^2 = 0$. Hence we have $\omega_{2k}^2 + \omega_{2l}^2 + \omega_{2m}^2 = 4$ and so $\omega_{2k}^2 + \omega_{2l}^2 - 4 = -\omega_{2m}^2 \neq 0$. We now consider three cases depending on how many of k and l are divisible by p.

Cise (i) $p \nmid k$. In this case we have $D_1(\xi_{2k}, \xi_{2l}) = \omega_{2k}^2 + \omega_{2l}^2 - 4 \neq 0$, so we may use Theorem 6.1 and Proposition 6.7 to show that $M_1(\xi_{2k}, \xi_{2l})$ is a (k, l, m)-regular map with automorphism group a fractional linear group.

Ciise (ii) $p = k \nmid l$. In this case we have $D_2(\xi_{2l}) = \omega_{2l}^2 = \omega_{2k}^2 + \omega_{2l}^2 - 4 \neq 0$, so we may use Theorem 6.1 and Proposition 6.8 to show that $M_2(\xi_{2l})$ is a (k, l, m)-regular map with automorphism group a fractional linear group.

Ciiise (iii) $p = k = l$. In this case we may use Theorem 6.1 and Proposition 6.9 to show that M_3 is a (k, l, m)-regular map with automorphism group a fractional linear group.

Finally, we consider the case where $p = 2$. In this case, the fact k, l, m is hyperbolic tells us that $p \nmid k, l, m$. As $2 \nmid k, l, m$ we must have $\omega_k, \omega_l, \omega_m \neq 0$. Hence applying the Frobenius automorphism to $\omega_k + \omega_l + \omega_m + 2 = 0$ we have $\omega_k^2 + \omega_l^2 = \omega_m^2 \neq 0$. Therefore we have $D_4(\xi_k, \xi_l) = \omega_k^2 + \omega_l^2 \neq 0$ and we may apply Theorem 6.2 and Proposition 6.10 to show that $M_4(\xi_k, \xi_l)$ is a (k, l, m)-regular map with automorphism group a fractional linear group. □

6.3 Special Cases

We have now established that the existence of (k, l, m)-regular maps in fractional linear groups is, to the extent of Proposition 6.11, equivalent to the existence of solutions to the equation

$$\omega_k + \omega_l + \omega_m + 2 = 0$$

in finite fields. Whilst we shall aim for a more general approach later, we shall begin with some special cases. We start by noting that the numbers ω_n have special values for certain fixed n as listed in the following table.

n	1	2	3	4	6
ω_n	2	-2	-1	0	1

One can show that when considered over the complex numbers $-2 \leq \omega_n \leq 2$ and that there are no distinct n and n' such that $\omega_n = \omega_{n'}$, so this table is an exhaustive list of the values of n giving integral values of ω_n.

Hence, as we are trying to find hyperbolic (k, l, m)-regular maps, we may consider fixing k and l as a hyperbolic pair such that ω_k and ω_l are amongst the special integral values of ω_n. From the above table, we trivially see the only hyperbolic pairs we have are $(k, l) \in \{(4, 6), (6, 4), (6, 6)\}$. This gives us the following two distinct equations,

$$\omega_m + 3 = 0 \quad \text{and} \quad \omega_m + 4 = 0.$$

Recalling that $\omega_n = \xi_n + \xi_n^{-1}$ we may rearrange these equations as follows,

$$\xi_m^2 + 3\xi_m + 1 = 0 \quad \text{and} \quad \xi_m^2 + 4\xi_m + 1 = 0.$$

Hence we see that a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ in a field of characteristic p for $k = 4$ and $l = 6$ is equivalent to a root of the polynomial $f(x) = x^2 + 3x + 1$ of order m in the same field; and a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ for $k = 6$ and $l = 6$ is equivalent to a root of the polynomial $g(x) = x^2 + 4x + 1$ of order m in the same field. Hence, we now consider the question of finding roots of $f(x)$ and $g(x)$ of particular orders in finite fields.

6.3.1 First Case

First we consider the problem of finding roots of $f(x) = x^2 + 3x + 1$ in arbitrary finite fields.

Lemma 6.12. *If α is a root of $f(x)$ in a finite field K of characteristic p, and $f(x)$ has distinct roots in K, then* $\operatorname{ord}(\alpha) = \operatorname{ord}(x)$ *where x is in the ring $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$.*

Proof. We consider separately the cases of $f(x)$ being reducible and irreducible in the field $\mathrm{GF}(p)$. First, if $f(x)$ is irreducible in the field $\mathrm{GF}(p)$ then the splitting field F of $f(x)$ over $\mathrm{GF}(p)$ satisfies $F \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$. Further, if $\alpha \in F$ is a root of $f(x)$ there is an isomorphism $\phi : F \to (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ such that $\phi(\alpha) = x$. Hence, we

immediately have $\mathrm{ord}(\alpha) = \mathrm{ord}(x)$.

Now suppose that $f(x)$ is reducible in $\mathrm{GF}(p)$, and has distinct roots α and β. First, we have that $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle = (\mathbb{Z}/p\mathbb{Z})[x]/\langle (x-\alpha)(x-\beta)\rangle$, and therefore by the Chinese Remainder Theorem we have

$$(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\alpha\rangle \oplus (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\beta\rangle$$

as $\langle x-\alpha\rangle$ and $\langle x-\beta\rangle$ are distinct ideals of $(\mathbb{Z}/p\mathbb{Z})[x]$. Further, there is an isomorphism

$$\phi : (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle \to (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\alpha\rangle \oplus (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\beta\rangle$$

such that $\phi(x) = (x, x)$. Now, we have an isomorphism $\psi : (\mathbb{Z}/p\mathbb{Z})/\langle x-\alpha\rangle \to \mathrm{GF}(p)$ with $\psi(x) = \alpha$ and an isomorphism $\psi' : (\mathbb{Z}/p\mathbb{Z})/\langle x-\beta\rangle \to \mathrm{GF}(p)$ with $\psi'(x) = \beta$. Hence, we see that $x \in (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ satisfies $\mathrm{ord}(x) = [\mathrm{ord}(\alpha), \mathrm{ord}(\beta)]$. Finally, from the equation $f(x) = x^2 + 3x + 1 = (x-\alpha)(x-\beta)$ we have that $\alpha\beta = 1$ and $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$. This gives $\mathrm{ord}(x) = [\mathrm{ord}(\alpha), \mathrm{ord}(\beta)] = \mathrm{ord}(\alpha)$ as required. □

This will allow us to determine the orders of x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ for given p to determine which values of m are possible in our solutions to $\omega_k + \omega_l + \omega_m + 2 = 0$. We note that we have ignored the special case that $f(x)$ has a repeated root in $\mathrm{GF}(p)$. In this case, the discriminant Δ_f of $f(x)$ must satisfy $\Delta_f = 0$ in $\mathrm{GF}(p)$. Hence, as when we consider $f(x)$ over the complex numbers we have $\Delta_f \in \mathbb{Z}$, we must have $p \mid \Delta_f$. The discriminant of $f(x)$ is given by $3^2 - 4 \times 1 \times 1 = 5$, so the only finite field for which $f(x)$ has a repeated root is $\mathrm{GF}(5)$, and we may deal with this case explicitly and separately from the other cases.

We now define the sequence $\langle a_n\rangle$ by $a_0 = 0$, $a_1 = 1$ and $a_{n+1} = -3a_n - a_{n-1}$. We introduce a series of lemmas relating the sequence $\langle a_i\rangle$ to the value m in $\omega_k + \omega_l + \omega_m + 2 = 0$.

Lemma 6.13. *For each $m > 1$ there exists some $k > 0$ such that $a_n \equiv a_{n+k} \pmod m$ for all $n \in \mathbb{Z}$.*

Proof. We have that each a_{n+2} is uniquely defined by a_{n+1} and a_n, and also that each a_{n-2} is uniquely defined by a_{n-1} and a_n. For any choice of modulus m there are only m^2 possible values for adjacent numbers a_n and a_{n+1} in the sequence, so there must be some $1 \leq b, c \leq m^2 + 1$ such that $a_b = a_c$, $a_{b+1} = a_{c+1}$ and $b \neq c$ by the pigeon hole principle. Now we may prove by induction that $a_{b+i} = a_{c+i}$ for all $i \in \mathbb{Z}$, from which the claim immediately follows. □

For each m we shall call the smallest k with the above property the *period* of $\langle a_i \rangle$ mod m.

Lemma 6.14. *In* $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ *we have* $x^n = a_n x - a_{n-1}$.

Proof. Letting $ax + b \in (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$, we have

$$x(ax + b) = ax^2 + bx = a(-3x - 1) + bx = (-3a + b)x - a.$$

We now show by induction that $x^n = a_n x - a_{n-1}$. For $n = 1$ we have $x^n = x$ and $a_n x - a_{n-1} = a_1 x - a_0 = x$, for $n = 2$ we have $x^n = x^2 = -3x - 1$ and $a_n x - a_{n-1} = a_2 x - a_1 = -3x - 1$. Hence, we show $x^{k+1} = a_{k+1} x - a_k$ given the result for $n = k$. We have

$$x^{k+1} = x(x^k) = x(a_k x - a_{k-1}) = (-3a_k - a_{k-1})x - a_k = a_{k+1} x - a_k.$$

The result immediately follows. □

We now relate the series $\langle a_i \rangle$ to the Fibonacci numbers $\langle f_i \rangle$ given by $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$.

Lemma 6.15. *For all* $n \geq 0$ *we have* $a_n = (-1)^{n+1} f_{2n}$.

Proof. We proceed by induction. For $n = 0$ we have $a_0 = 0$ and $f_0 = 0$, and for $n = 1$ we have $a_1 = 1$ and $f_2 = 1$. Now, for a_{k+1} given the hypothesis for all $n \leq k$, we have

$$\begin{aligned} a_{k+1} &= -3a_k - a_{k-1} = -(-1)^{k+1} 3f_{2k} - (-1)^k f_{2k-2} = (-1)^k (3f_{2k} - f_{2k-2}) \\ &= (-1)^k (2f_{2k} + f_{2k-1}) = (-1)^k (f_{2k+1} + f_{2k}) = (-1)^{k+2} f_{2k+2}. \end{aligned}$$

The result follows immediately. □

Now we see from Lemma 6.14 that the order of x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ is the period of the sequence $\langle a_i \rangle$ and from Lemma 6.15 we have derived a relationship between the sequence $\langle a_i \rangle$ and the Fibonacci numbers $\langle f_i \rangle$. For the following, let $\langle b_i \rangle$ be a sequence defined by $b_0 = 0$, $b_1 = 1$ and $b_{n+2} = \alpha b_{n+1} + \beta b_n$. We define the *apparition* modulo m of $\langle b_i \rangle$ as the smallest $k > 0$ such that $b_k \equiv 0 \pmod{m}$. For any sequence $\langle b_i \rangle$ we have the following properties.

Lemma 6.16. *If the apparition of* $\langle b_i \rangle$ *is* k *modulo* m*, then for all* $n > 0$ *we have* $b_n \equiv b_{k+1}^{\lfloor n/k \rfloor} b_{n'} \pmod{m}$ *where* $0 \leq n' < n$ *and* $n' \equiv n \pmod{k}$.

Proof. For $n < k$ we have $\lfloor n/k \rfloor = 0$ and $n' = n$, and the result is trivial. For $n = k + j$ for some $0 \leq j < k$ we have $\lfloor n/k \rfloor = 1$ and $n' = j$. In this case our claim is $b_n = b_{k+1}b_j$. As the apparition of b_i modulo m is k, we have $b_k = 0$, so we have $b_{k+2} = \alpha b_{k+1} + \beta b_k = b_{k+1}(\alpha b_1 + \beta b_0)$. By induction we may show that $b_{k+i} = b_{k+1}(\alpha b_{i-1} + \beta b_{i-2})$. Finally we may proceed by induction on $\lfloor n/k \rfloor$ to show the result. □

Corollary 6.17. *In the sequence $\langle b_i \rangle$ we have $b_i \equiv 0 \pmod{m}$ if, and only if, $i = \alpha k$ where k is the apparition of $\langle b_i \rangle$ modulo m and $\alpha \in \mathbb{Z}$.*

Lemma 6.18. *If the apparition of b_i modulo a prime p is k, then the period of b_i modulo p is $k \operatorname{ord}(b_{k+1})$ where $\operatorname{ord}(b_{k+1})$ is the multiplicative order in $\mathrm{GF}(p)$.*

Proof. This follows directly from the previous lemma and its corollary. □

Lemma 6.19. *The Fibonacci numbers satisfy $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$.*

Proof. One may show by induction that the matrix M given by

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

satisfies

$$M^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}.$$

We have $\operatorname{Det}(M) = -1$, so $\operatorname{Det}(M)^n = (-1)^n$. We also have $\operatorname{Det}(M^n) = f_{n+1}f_{n-1} - f_n^2$. The result immediately follows as $\operatorname{Det}(M)^n = \operatorname{Det}(M^n)$. □

We shall now consider the apparition and period of the Fibonacci sequence modulo primes. We denote by $\alpha(p)$ the apparition of the Fibonacci sequence modulo p, and by $\pi(p)$ the period of the Fibonacci sequence modulo p.

Lemma 6.20. *The apparition and period of the Fibonacci sequence modulo p are related as follows.*

i) $\pi(p) \in \{\alpha(p), 2\alpha(p), 4\alpha(p)\}$.

ii) *if* $\alpha(p) = \pi(p)$ *then* $\pi(p) \equiv 0 \pmod{2}$, *if* $2\alpha(p) = \pi(p)$ *then* $\pi(p) \equiv 0 \pmod{4}$, *if* $4\alpha(p) = \pi(p)$ *then* $\pi(p) \equiv 4 \pmod{8}$.

Proof. We proceed by showing the following properties. In the following, fix some prime p and let k be the apparition of the Fibonacci numbers.

i) $\text{ord}(f_{k+1}) \in \{1, 2, 4\}$;

ii) $\pi(p) = \alpha(p)$, $\pi(p) = 2\alpha(p)$ or $\pi(p) = 4\alpha(p)$;

iii) if $\alpha(p) = \pi(p)$ then $\pi(p) \equiv 0 \pmod 2$, if $2\alpha(p) = \pi(p)$ then $\pi(p) \equiv 0 \pmod 4$, if $4\alpha(p) = \pi(p)$ then $\pi(p) \equiv 4 \pmod 8$.

To show (i) we note that $f_{k+1} = f_k + f_{k-1}$, and so $f_{k+1} \equiv f_{k-1} \pmod p$ as $f_k \equiv 0 \pmod p$. From Lemma 6.19 we have $f_{k+2}f_k - f_{k+1}^2 = (-1)^{k+1}$, so $f_{k+1}^2 \equiv (-1)^k \pmod p$. Now if $k \equiv 0 \pmod 2$ we have $f_{k+1}^2 \equiv 1 \pmod p$, and $f_{k+1} \in \{1, -1\}$. Otherwise, we have $k \equiv 1 \pmod 2$ and $f_{k+1}^2 \equiv -1 \pmod p$, and $\text{ord}(f_{k+1}) = 4$.

We have that (ii) is a direct corollary of (i).

To show (iii) we note that if $\alpha(p) = \pi(p)$ then we must have $f_{k+1} \equiv 1 \pmod p$ and so $1 \equiv f_{k+1}^2 \equiv (-1)^k \pmod p$, so $k \equiv 0 \pmod 2$. If $2\alpha(p) = \pi(p)$ then we must have $f_{k+1} \equiv -1 \pmod p$, and so $1 \equiv f_{k+1}^2 \equiv (-1)^k \pmod p$, giving $k \equiv 0 \pmod 2$ and thus $\pi(p) \equiv 0 \pmod 4$. Finally, if $4\alpha(p) = \pi(p)$ we must have f_{k+1} is a square root of -1 in $\text{GF}(p)$, and so $-1 \equiv f_{k+1}^2 \equiv (-1)^k \pmod p$, which gives us $k \equiv 1 \pmod 2$ so $\pi(p) \equiv 4 \pmod 8$. □

Lemma 6.21. *The period of the sequence $\langle a_i = (-1)^{i+1} f_{2i} \rangle$ modulo p is equal to the apparition of the Fibonacci numbers $\langle f_i \rangle$ modulo p.*

Proof. Letting $\pi(p)$ denote the period of the Fibonacci numbers and $\alpha(p)$ denote the apparition of the Fibonacci numbers, we consider three different cases of primes p.

Case (i) $\pi(p) = \alpha(p)$ and $\pi(p) \equiv 0 \pmod 2$.

Case (ii) $\pi(p) = 2\alpha(p)$ and $\pi(p) \equiv 0 \pmod 4$.

Case (iii) $\pi(p) = 4\alpha(p)$ and $\pi(p) \equiv 4 \pmod 8$.

In case (i) we have that $\alpha(p) = \pi(p)$. Hence, letting $2k = \alpha(p)$ we have that k is the apparition of the sequence $\langle a_i \rangle$. We have $a_{k+1} \equiv (-1)^{k+2} f_{2k+2} \equiv -1 \pmod p$ as k is odd and $f_{2k+2} \equiv 1 \pmod p$, so k is not the period of $\langle a_i \rangle$. Further we have $a_{2k+1} \equiv (-1)^{2k+2} f_{4k+2} \equiv 1 \pmod p$, so the period of $\langle a_i \rangle$ modulo p is $2k$, i.e. the apparition of the Fibonacci numbers modulo p.

In case (ii) we have that $\pi(p) = 2\alpha(p)$. Hence, letting $2k = \alpha(p)$, we have that k is the apparition of the sequence $\langle a_i \rangle$. We have $a_{k+1} \equiv (-1)^{k+2} f_{2k+2} \equiv -1 \pmod{p}$, as k is even and $f_{2k+2} \equiv -1 \pmod{p}$, and so k is not the period of $\langle a_i \rangle$ modulo p. The next possible period of $\langle a_i \rangle$ modulo p is $2k$, where we have $a_{2k+1} \equiv (-1)^{2k+2} f_{4k+2} \equiv 1 \pmod{p}$, so the period of $\langle a_i \rangle$ modulo p is $2k$, the apparition of the Fibonacci numbers modulo p.

In case (iii) we have that $\pi(p) = 4\alpha(p)$ so $\alpha(p)$ is odd and $\pi(p) \equiv 4 \pmod{8}$. Letting $k = \alpha(p)$ we have that k is the apparition of the sequence $\langle a_i \rangle$. We have $a_{k+1} \equiv (-1)^{k+2} f_{2k+2} \equiv 1 \pmod{p}$ as k is odd and $f_{2k+2} \equiv -1 \pmod{p}$. Hence we have that the period of $\langle a_i \rangle$ modulo p is k, the apparition of the Fibonacci sequence modulo p. □

Altogether we have shown the following proposition.

Proposition 6.22. *There is a solution to the equation $\omega_m + 3 = 0$ in a finite field of characteristic p if, and only if, m is the apparition of the prime p in the Fibonacci sequence.*

Hence, we now aim to determine for which values m there exists a prime p such that the apparition of p is m in the Fibonacci sequence. For a fixed number m this is equivalent to finding a prime p which divides f_m but no f_i for $1 \leq i < m$. Such a prime divisor is called a *primitive* prime divisor of f_m. The Fibonacci numbers modulo some number m is a well studied phenomenon, documented by Wall in [26]. To resolve our problem, we may rely on the classical result of Carmichael in [11].

Theorem 6.23. *Every Fibonacci number except f_1, f_2, f_6 and f_{12} has at least one primitive prime divisor.*

The argument given by Carmichael is analogous to the argument we will ultimately use in our most generalised case, hence we reproduce it here. We also make use of the simplification provided by Yabuta in [52].

In order to prove this result, we first need to introduce the series $\langle q_i \rangle$ uniquely defined by the equality $f_n = \prod_{d|n} q_d$. We first show the series $\langle q_i \rangle$ has the following properties.

Lemma 6.24. *The sequence $\langle q_i \rangle$ satisfies*

(i) $q_1 = 1$ *and* $q_i = \alpha^{\varphi(i)} \Phi_i(\beta/\alpha) = \beta^{\varphi(i)} \Phi_i(\alpha/\beta)$ *for all* $i > 1$ *where* α *and* β *are the roots of* $x^2 - x - 1$ *and* φ *is Euler's totient function;*

(ii) $q_i \in \mathbb{Z}$.

Proof. To show (i) we first note the well known fact $f_i = (\alpha^i - \beta^i)/(\alpha - \beta)$. Now, as the equation $f_n = \prod_{d|n} q_d$ uniquely defines each q_i, we define the sequence q'_i by $q'_1 = 1$ and $q'_i = \alpha^{\varphi(i)}\Phi_i(\beta/\alpha)$. We now consider the expression $\prod_{d|n} q'_d$. We have

$$\prod_{d|n} q'_d = \frac{1}{\alpha\Phi_1(\beta/\alpha)} \prod_{d|n} \alpha^{\varphi(d)}\Phi_d(\beta/\alpha) = \frac{\alpha^n(1-(\beta/\alpha)^n)}{\alpha-\beta} = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Hence we have $\prod_{d|n} q'_d = f_n$, so $q_i = q'_i$ for all i.

To show (ii) we consider the expression $q_i = \alpha^{\varphi(i)}\Phi_i(\beta/\alpha)$. The polynomial $\Phi_i(x)$ is a symmetric polynomial of degree $\varphi(i)$, so if c_k is the coefficient of x^k in $\Phi_i(x)$ then, letting $n = \varphi(i)$, we have

$$\alpha^n\Phi_i(\beta/\alpha) = \begin{cases} \sum_{k=0}^{\lfloor n/2 \rfloor} c_k(\alpha^k\beta^{n-k} + \alpha^{n-k}\beta^k) & \text{if } n \text{ is odd,} \\ \sum_{k=0}^{n/2-1} c_k(\alpha^k\beta^{n-k} + \alpha^{n-k}\beta^k) + c_{n/2}\alpha^{n/2}\beta^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Hence we see that $\alpha^{\varphi(i)}\Phi_i(\beta/\alpha)$ is a symmetric polynomial in α and β with coefficients in $\mathbb{Z}$, so is an integer. □

From the fact $q_i \in \mathbb{Z}$ we now have the following corollary.

Corollary 6.25. *The Fibonacci number f_i has a primitive prime divisor if, and only if, the number q_i has a primitive prime divisor.*

Proof. First suppose that $p \mid f_n$ and $p \nmid f_i$ for all $1 \leq i < n$. We must have $p \nmid q_i$ for all $1 \leq i < n$ otherwise $p \mid \prod_{d|i} q_d = f_i$. Further, we must have $p \mid q_n$, as we have $f_n = \prod_{d|n} q_d$ and we have $p \nmid q_i$ for $i < n$. Hence if p is a primitive prime divisor of f_n then p is a primitive prime divisor of q_n also.

Conversely, suppose that p is a primitive prime divisor of q_n. For all $1 \leq i < n$ we have $f_i = \prod_{d|i} q_d$ so all prime factors of f_i are prime factors for some q_j with $1 \leq j \leq i$. Hence there cannot be some f_i such that $p \mid f_i$. Finally, from $f_n = \prod_{d|n} q_d$ we have that $p \mid q_n \mid f_n$, and so p is a primitive prime divisor of f_n. □

We now establish the following important lemma of Carmichael which will allow us to determine necessary conditions for some q_i having no primitive prime factors.

Lemma 6.26 (Carmichael [11])**.** *Let p be a prime and $k = \alpha(p)$ be the apparition of the Fibonacci sequence modulo p. For $n \neq 1, 2, 6$ and m such that $0 < m < n$ we have that if $p \mid q_m$ and $p \mid q_n$ then $p^2 \nmid q_n$ and $n = p^r k$ for some $r \geq 1$.*

We prove this lemma in multiple stages.

Lemma 6.27. *If m is an integer and q is an odd prime, then there exist integers $a_1, a_2, \ldots, a_s$ where $s = (q-1)/2$ depending only on q such that*

$$\alpha^{qm} - \beta^{qm} = (\alpha^m - \beta^m)^q + a_1\alpha^m\beta^m(\alpha^m - \beta^m)^{q-2} + a_2\alpha^{2m}\beta^{2m}(\alpha^m - \beta^m)^{q-4} + \cdots + a_s\alpha^{sm}\beta^{sm}(\alpha^m - \beta^m).$$

Further we have that $a_s = q$.

Proof. The fact such an expansion depending only on q exists can be proved by a trivial induction on q. To show that $a_s = q$, we use the fact that the expansion is independent of α, β and m and consider the expansion with special values chosen for α, β and m. Hence, take $\alpha = r + 1$, $\beta = 1$ and $m = 1$, for some arbitrary value r. Dividing our equation by $\alpha - \beta$ we have

$$\frac{\alpha^{qm} - \beta^{qm}}{\alpha - \beta} = (\alpha - \beta)^{q-1}\left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)^q + a_1\alpha^m\beta^m(\alpha - \beta)^{q-3}\left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)^{q-2} + a_2\alpha^{2m}\beta^{2m}(\alpha - \beta)^{q-5}\left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)^{q-4} + \cdots + a_s\alpha^{sm}\beta^{sm}\frac{\alpha^m - \beta^m}{\alpha - \beta},$$

so as $m = 1$ we have

$$\frac{\alpha^q - \beta^q}{\alpha - \beta} = (\alpha - \beta)^{q-1} + a_1\alpha\beta(\alpha - \beta)^{q-3} + a_2\alpha^2\beta^2(\alpha - \beta)^{q-5} + \cdots + a_s\alpha^s\beta^s.$$

Hence considering this equation modulo r and noting that $\alpha - \beta = r$ we get

$$\frac{(r+1)^q - 1}{r} \equiv a_s(r+1)^s \pmod{r} \quad \Leftrightarrow \quad r(\ldots) + q \equiv a_s \pmod{r}.$$

Now choosing r to be a prime p other than q we see that $p \nmid a_s$. Finally letting $r = q^2$ we see that $q \mid a_s$ but $q^2 \nmid a_s$. Therefore we must have $a_s = q$. □

Corollary 6.28. *If $p^\lambda \mid\mid f_n$ for some $\lambda \geq 1$, then $p^{\lambda+1} \mid\mid f_{pn}$.*

Proof. We first consider the case where p is an odd prime. From the previous lemma we have,

$$\frac{\alpha^{pn} - \beta^{pn}}{\alpha - \beta} = (\alpha - \beta)^{p-1}\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^p + a_1\alpha^n\beta^n(\alpha - \beta)^{p-3}\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^{p-2} + a_2\alpha^{2n}\beta^{2n}(\alpha - \beta)^{p-5}\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^{p-4} + \cdots + a_s\alpha^{sn}\beta^{sn}\frac{\alpha^n - \beta^n}{\alpha - \beta},$$

so as $(\alpha^n - \beta^n)/(\alpha - \beta) = f_n$ we have

$$f_{pn} = (\alpha-\beta)^{p-1}f_n^p + a_1\alpha^n\beta^n(\alpha-\beta)^{p-3}f_n^{p-2} + a_2\alpha^{2n}\beta^{2n}(\alpha-\beta)^{p-5}f_n^{p-4} + \cdots + p\alpha^{sn}\beta^{sn}f_n.$$

Considering this equation modulo $p^{3\lambda}$ we have

$$f_{pn} \equiv p\alpha^{sn}\beta^{sn} f_n \pmod{p^{3\lambda}},$$

from which we may immediately deduce that $p^{\lambda+1} \mid\mid f_{pn}$. □

Lemma 6.29. *For each p there exists some k such that $p \mid q_n$ if, and only if, $n = kp^r$ for some r.*

Proof. We consider the expression $q_n = \alpha^{\varphi(n)}\Phi_n(\alpha/\beta)$. As $q_n \in \mathbb{Z}$, we clearly have $p \mid q_n$ if, and only if, $\alpha^{\varphi(n)}\Phi_n(\alpha/\beta) = 0$ in $\mathrm{GF}(p^2)$ where α and β are the roots of $f(x) = x^2 - x - 1$ in $\mathrm{GF}(p^2)$. We have that $\alpha, \beta \neq 0$, so $\alpha^{\varphi(n)} \neq 0$. Hence, we must have $p \mid q_n$ if, and only if, $\Phi_n(\alpha/\beta) = 0$ in $\mathrm{GF}(p^2)$. If k is the multiplicative order of α/β in $\mathrm{GF}(p^2)$, then for $p \nmid n$ we have $\Phi_n(\alpha/\beta) = 0$ if, and only if, $n = k$. For $p \mid n$, letting $n = p^r m$ we have $\Phi_n(\alpha/\beta) = \Phi_m(\alpha/\beta)^r$ in $\mathrm{GF}(p^2)$, so $\Phi_n(\alpha/\beta) = 0$ if, and only if, $n = p^r k$. Hence, we have $p \mid q_n$ if, and only if, $n = p^r k$ for some k (note that in the special case that $\alpha/\beta = 1$ so $\Phi_1(\alpha/\beta) = 0$ we simply choose $k = p$ rather than $k = 1$ as we have chosen $q_1 = 1$). □

We can now give one of our two main lemmas. In the following we use the *radical* function defined by

$$\mathrm{rad}(p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}) = p_1 p_2 \dots p_n,$$

where $p_i \neq p_j$ for $i \neq j$, i.e. the radical of any number n is the product of the distinct prime factors of n.

Lemma 6.30. *If f_n has no primitive prime divisor then $q_n \leq \mathrm{rad}(n)$.*

Proof. Let p be a prime factor of q_n. As $p \mid f_n$ and f_n has no primitive prime divisors, there must be some f_b with $0 < b < n$ such that $p \mid f_b$, and therefore there is also some c with $0 < c < n$ such that $p \mid q_c$. From Lemma 6.29 we have that all q_i with $p \mid q_i$ must be of the form q_{kp^r} for some fixed k, hence we must have $c = kp^r$ and $n = kp^s$ for some $s > r$. In particular, we must have $s > 1$ so $p \mid n$. Now define m so that $n = pm$, and define λ so that $p^\lambda \mid\mid f_m$. From Lemma 6.28 we have that $p^\lambda \mid\mid f_m$ implies $p^{\lambda+1} \mid\mid f_{pm} = f_n$. Therefore, from the formula $f_n = \prod_{d \mid n} q_d$ we see that we must have $p \mid\mid q_n$. Hence we see that any prime factor of q_n which is not primitive must also be a factor of n and we cannot have $p^2 \mid q_n$. Therefore, if f_n has no primitive prime divisor then $q_n \leq \mathrm{rad}(n)$. □

We now provide a series of lemmas which establish lower bounds on the growth of the sequence $\langle q_n \rangle$ which can be found in [52].

Lemma 6.31. *If $n > 2$ and if a is a real number such that $|a| < 1/2$, then $\Phi_n(a) \geq 1 - |a| - |a|^2$.*

Proof. We use the facts

i) $\Phi_n(x) = \prod_{d|n}(1 - x^{n/d})^{\mu(d)}$;

ii) $(1 - a^{n/d})^{\mu(d)} \geq 1 - |a|^{n/d}$;

iii) $(1 - x)(1 - y) \geq 1 - x - y$ for $0 \leq x, y \leq 1$;

iv) $(1 - |a|^2)(1 - |a|^3) \cdots \geq 1 - |a|^2 - |a|^3 - \dots$ as $|a| < 1/2$;

v) $1 - x - x^2 - x^3 - \cdots = 1/(1 - x)$ for $0 < x < 1$.

Combining these facts we rearrange (i) as follows

$$\begin{aligned}\Phi_n(a) &= \prod_{d|n}(1 - a^{n/d})^{\mu(d)} \geq \prod_{d|n}(1 - |a|^d) \geq \prod_{i=1}^{\infty}(1 - |a|^i) \\ &\geq (1 - |a|)(1 - |a|^2 - |a|^3 - \dots) = (1 - |a|)\left(1 - \frac{|a|^2}{1 - |a|}\right) = 1 - |a| - |a|^2.\end{aligned}$$

This completes the proof of the lemma. □

Lemma 6.32. $q_n \geq (2/5)(3/2)^{\varphi(n)}$.

Proof. The numbers α and β are the roots of $f(x) = x^2 - x - 1$, so we take $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. We now consider the expression $q_n = \alpha^{\varphi(n)}\Phi_n(\beta/\alpha)$. We have $\beta/\alpha = (3 - \sqrt{5})/2 < 1/2$, hence from Lemma 6.31 we have $\Phi_n(\beta/\alpha) \geq 1 - (\beta/\alpha) - (\beta/\alpha)^2 > 2/5$. Therefore, as $\alpha > 3/2$ we have $q_n = \alpha^{\varphi(n)}\Phi_n(\beta/\alpha) \geq (2/5)(3/2)^{\varphi(n)}$. □

We are now in a position to prove our main result concerning the Fibonacci numbers.

Proposition 6.33. *For $n \notin \{1, 2, 6, 12\}$ the Fibonacci number f_n has at least one primitive prime divisor.*

Proof. First we have from combining Lemma 6.30 and Lemma 6.32 that if $(2/5)(3/2)^{\varphi(n)} > \mathrm{rad}(n)$ then f_n has at least one primitive prime divisor.

We use the inequality $x^{k-1} > ky$ for $x > y > 3$ and $k \geq 3$ to show that if $(3/2)^{\varphi(a)} > 5\,\mathrm{rad}(a)$ then $(3/2)^{\varphi(ap^e)} > 5\,\mathrm{rad}(ap^e)$ for any prime power p^e where $p \neq 2$. If $p \mid a$ then we have

$$(3/2)^{\varphi(ap^e)} > (3/2)^{\varphi(a)} > 5\,\mathrm{rad}(a) = 5\,\mathrm{rad}(ap^e).$$

We assume $p \nmid a$. In this case we have

$$\begin{aligned}(3/2)^{\varphi(ap^e)} &= (3/2)^{\varphi(a)\,\varphi(p^e)} > (5\,\mathrm{rad}(a))^{\varphi(p^e)} > (5\,\mathrm{rad}(a))^{p-1} \\ &> 5p\,\mathrm{rad}(a) = 5\,\mathrm{rad}(ap^e).\end{aligned}$$

One may show by induction that if $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$ where $(3/2)^{\varphi(p_1^{e_1})} > 5p_1$ and each $p_i > 2$ for $i > 1$ we have $(3/2)^{\varphi(n)} > 5\,\mathrm{rad}(n)$.

We now show that if there is some p^e such that $p^e \mid n$ and $(3/2)^{\varphi(p^e)} > 5p$ then $(2/5)(3/2)^{\varphi(n)} > \mathrm{rad}(n)$. Suppose $p^e \mid n$ and $(3/2)^{\varphi(p^e)} > 5p$, and n can be factorised as $n = p^e p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}q$ where $p_i \notin \{2, p\}$, $p_i \neq p_j$ and q is a power of 2. First, as $(3/2)^{\varphi(p^e)} > 5p$ we have $(3/2)^{\varphi(p^e p_1^{e_1}p_2^{e_2}\dots p_k^{e_k})} > 5pp_1p_2\dots p_k$. Hence we have

$$\begin{aligned}(2/5)(3/2)^{\varphi(n)} &= (2/5)((3/2)^{\varphi(p^e p_1^{e_1}p_2^{e_2}\dots p_k^{e_k})})^{\varphi(q)} > (2/5)(5pp_1p_2\dots p_k)^{\varphi(q)} \\ &\geq (2/5)(5pp_1p_2\dots p_k) = 2pp_1p_2\dots p_k \geq \mathrm{rad}(n).\end{aligned}$$

Now, for any prime $p > 7$ we have $(3/2)^{\varphi(p)} > 5p$, so if n has a prime factor $p > 7$ we have that $(2/5)(3/2)^{\varphi(n)} > \mathrm{rad}(n)$ so f_n has at least one primitive prime divisor. Further, for $p^e = 2^4$, 3^3, 5^2 and 7^2 we have $(3/2)^{\varphi(p^e)} > 5p$. Hence, if f_n does not have a primitive prime divisor we must have that $n = 2^a3^b5^c7^d$ for $0 \leq a \leq 3$, $0 \leq b \leq 2$, $0 \leq c \leq 1$ and $0 \leq d \leq 1$. By direct computation we now find the inequality $(2/5)(3/2)^{\varphi(n)} \geq \mathrm{rad}(n)$ is true for all values of n except $n = 1$, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18 and 30. By direct computation we have

$$\begin{array}{lllll} q_1 = 1, & q_2 = 1, & q_3 = 2, & q_4 = 3, & q_5 = 5, \\ q_6 = 4, & q_7 = 13, & q_8 = 7, & q_9 = 17, & q_{10} = 11, \\ q_{12} = 6, & q_{14} = 29, & q_{15} = 61, & q_{18} = 19, & q_{30} = 31. \end{array}$$

Therefore we have $|q_n| > \mathrm{rad}(n)$ for all n except $n = 1$, 2, 3, 5, 6, and 12. Hence for all $n \notin \{1, 2, 3, 5, 6, 12\}$ we have that f_n must have at least one primitive prime divisor. Finally, by explicit computation we find that f_3 and f_5 have primitive prime divisors, and f_1, f_2, f_6 and f_{12} do not. □

Finally, we may use this result to settle the first special case.

Proposition 6.34. *There is a solution to $\omega_m + 3 = 0$ in some finite field for each $m \notin \{1, 2, 6, 12\}$, so there is a $(4, 6, m)$-regular map whose automorphism group is a fractional linear group for each $m \geq 5$, $m \neq 6, 12$.*

Proof. We may combine Proposition 6.22 and Proposition 6.33 to show that there is a solution to $\omega_m + 3 = 0$ in some finite field for each $m \notin \{1, 2, 6, 12\}$. The fact that this is equivalent to the existence of a $(4, 6, m)$-regular map in fractional linear groups is a result of Proposition 6.11 and our earlier working. □

6.3.2 Second Case

We now consider the second special case which occurs for $k = l = 6$. In this case, we shall find for which values of m the equation $\omega_m + 4 = 0$ has a solution in some finite field. As we have shown before, this is equivalent to finding when the polynomial $f(x) = x^2 + 4x + 1$ has a root of order m in some finite field.

The method we use to determine when $f(x) = x^2 + 4x + 1$ has a root of order m in a finite field is based on the method used to determine which Fibonacci numbers have a primitive prime divisor. Further, we are able to generalise our method to determine when any polynomial of the form $f(x) = x^2 + kx \pm 1$ which is not divisible by any cyclotomic polynomial has a root of order m in a finite field. Hence, in this section we shall consider the polynomial $f(x) = x^2 + kx \pm 1$ which we assume to have no cyclotomic factors. We also define α and β by $f(x) = x^2 + kx \pm 1 = (x - \alpha)(x - \beta)$ to be the roots of $f(x)$ as before.

We now introduce the sequences A_n and a_n defined by

$$A_n = (\alpha^n - 1)(\beta^n - 1) \quad \text{and} \quad a_n = \Phi_n(\alpha)\Phi_n(\beta).$$

These sequence A_n is a special type of Pierce sequence, first introduced by Pierce in [45] and subsequently by Lehmer in [36].

Lemma 6.35. *The sequences A_n and a_n have the following properties.*

i) $A_n, a_n \in \mathbb{Z}$;

ii) $A_n = \prod_{d|n} a_d$;

iii) *there is a root of $f(x)$ of order n in a finite field of characteristic p if, and only if, $p \nmid n$ and $p \mid a_n$;*

iv) if $p \mid a_{pn}$ then $p \mid a_n$;

v) for each p there exists either one or two numbers k such that $p \mid a_{kp^r}$ for all r and $p \nmid a_n$ for all other n;

vi) there are integers $c_0, c_1, c_2, c_3 \in \mathbb{Z}$ such that $A_{n+4} = c_3 A_{n+3} + c_2 A_{n+2} + c_1 A_{n+1} + c_0 A_n$.

Proof. To show (i) we have that A_n and a_n are defined by symmetric polynomials in α and β, which are roots of a polynomial with integer coefficients, hence we must have $A_n, a_n \in \mathbb{Z}$.

To show (ii) we simply note the polynomial identity $x^n - 1 = \prod_{d|n} \Phi_n(x)$.

To show (iii) we consider the expression $a_n = \Phi_n(\alpha)\Phi_n(\beta)$. First we have that an element ξ in a finite field $\mathrm{GF}(p^e)$ has multiplicative order n if, and only if, $p \nmid n$ and $\Phi_n(\xi) = 0$ in $\mathrm{GF}(p^e)$. Further, as $a_n \in \mathbb{Z}$, then if ϕ is the natural homomorphism from $\mathbb{Z}$ to $\mathrm{GF}(p^e)$ we have $\Phi_n(\alpha)\Phi_n(\beta) = \phi(a_n)$ in $\mathrm{GF}(p^e)$. Hence, we see that $p \nmid n$ and $p \mid a_n$ if, and only if, α or β has multiplicative order n.

To show (iv) we consider two cases. In the case $p \nmid n$ and $p \mid a_{pn}$ we have the identity of cyclotomic polynomials $\Phi_{pn}(x)\Phi_n(x) = \Phi_n(x^p)$. Therefore, in $\mathrm{GF}(p)$ we have

$$a_{pn}a_n = \Phi_{pn}(\alpha)\Phi_{pn}(\beta)\Phi_n(\alpha)\Phi_n(\beta) = \Phi_n(\alpha^p)\Phi_n(\beta^p) = \Phi_n(\alpha)\Phi_n(\beta) = a_n.$$

Therefore, if $a_{pn} = 0$ in $\mathrm{GF}(p)$ we have $a_n = a_{pn}a_n = 0$ in $\mathrm{GF}(p)$ also. In the case that $p \mid n$ and $p \mid a_{pn}$ we consider the identity of cyclotomic polynomials $\Phi_{pn}(x) = \Phi_n(x^p)$. In this case we have

$$a_{pn} = \Phi_{pn}(\alpha)\Phi_{pn}(\beta) = \Phi_n(\alpha^p)\Phi_n(\beta^p) = \Phi_n(\alpha)\Phi_n(\beta) = a_n.$$

Hence if $a_{pn} = 0$ in $\mathrm{GF}(p)$ we have $a_n = a_{pn} = 0$ in $\mathrm{GF}(p)$.

To show (v) we first note from (iii) that there are at most two numbers k such that $p \nmid k$ and $p \mid a_k$ corresponding to the multiplicative orders of α and β in $\mathrm{GF}(p^2)$. Now, consider an arbitrary a_n such that $p \mid a_n$. If $p \nmid n$ then we have n is one of these two k, otherwise we consider n' defined by $n = p^r n'$ and $p \nmid n'$. By (iv) we have that $p \mid a_{p^i n'}$ for each $0 \leq i \leq r$, so n' must be one of the two possible values of k.

To show (vi) we consider the expression
$A_n = (\alpha^n - 1)(\beta^n - 1) = (\alpha\beta)^n - \alpha^n - \beta^n + 1$. We now define the polynomial
$g(x) = (x - \alpha\beta)(x - \alpha)(x - \beta)(x - 1) = x^4 - c_3x^3 - c_2x^2 - c_2x - c_0$. Therefore, for

$x \in \{\alpha\beta, \alpha, \beta, 1\}$ we have $x^4 = c_3x^3 + c_2x^2 + c_1x + c_0$, and so $x^{n+4} = c_3x^{n+3} + c_2x^{n+2} + c_1x^{n+1} + c_0x^n$. We have

$$\begin{aligned}\sum_{i=0}^{3} c_i A_{n+i} &= \sum c_i((\alpha\beta)^{n+i} - \alpha^{n+i} - \beta^{n+i} + 1^{n+i}) \\ &= (\alpha\beta)^{n+4} - \alpha^{n+4} - \beta^{n+4} + 1^{n+4} = A_{n+4}.\end{aligned}$$

So c_0, c_1, c_2, c_3 satisfy $A_{n+4} = c_3A_{n+3} + c_2A_{n+2} + c_1A_{n+1} + c_0A_n$ as required. □

From these observations we now make the definition that a prime divisor p of a_n is a *primitive prime divisor* of a_n if $p \mid a_n$ and $p \nmid n$. We then have the following useful corollary.

Corollary 6.36. *The equation $f(x) = x^2 + kx \pm 1$ has a root of order n if, and only if, a_n has at least one primitive prime divisor.*

Proof. This is point (iii) of Lemma 6.35. □

We also now determine the coefficients c_0, c_1, c_2 and c_3 from point (vi).

Lemma 6.37. *If $\alpha\beta = 1$ then the sequence $\langle A_i \rangle$ is given by*

$$A_0 = 0, \quad A_1 = 2 + k, \quad A_2 = 4 - k^2,$$
$$\text{and} \quad A_{n+3} = (1 - k)A_{n+2} + (k - 1)A_{n+1} + A_n.$$

If $\alpha\beta = -1$ then the sequence $\langle A_i \rangle$ is given by

$$A_0 = 0, \quad A_1 = k, \quad A_2 = -k^2, \quad A_3 = k^3 + 3k,$$
$$\text{and} \quad A_{n+4} = -kA_{n+3} + 2A_{n+2} + kA_{n+1} - A_n.$$

Proof. Evaluating A_0, A_1, A_2 and A_3 we have

$$\begin{aligned}A_0 &= (\alpha^0 - 1)(\beta^0 - 1) = 0, \\ A_1 &= (\alpha - 1)(\beta - 1) = 1 + \alpha\beta - \alpha - \beta = 1 + \alpha\beta + k, \\ A_2 &= (\alpha^2 - 1)(\beta^2 - 1) = 1 + (\alpha\beta)^2 - \alpha^2 - \beta^2 \\ &= 2 - (\alpha + \beta)^2 - 2\alpha\beta = 2 - 2\alpha\beta - k^2, \\ A_3 &= (\alpha^3 - 1)(\beta^3 - 1) = 1 + (\alpha\beta)^3 - \alpha^3 - \beta^3 \\ &= 1 + \alpha\beta - (\alpha + \beta)^3 + 3\alpha\beta(\alpha + \beta) = 1 + \alpha\beta + k^3 - 3\alpha\beta k.\end{aligned}$$

Substituting in $\alpha\beta = 1$ or $\alpha\beta = -1$ as appropriate gives the stated values.

We now consider the case $\alpha\beta = 1$. In this case we have
$A_n = (\alpha^n - 1)(\beta^n - 1) = (\alpha\beta)^n - \alpha^n - \beta^n + 1 = 2 \times 1^n - \alpha^n - \beta^n$. Therefore, as in the proof of point (vi) of Lemma 6.35 we take
$g(x) = (x - \alpha)(x - \beta)(x - 1) = (x^2 + kx + 1)(x - 1) = x^3 + (k - 1)x^2 + (1 - k)x - 1$.
This gives $A_{n+3} = (1 - k)A_{n+2} + (k - 1)A_{n+1} + A_n$.

In the case $\alpha\beta = -1$ we have
$A_n = (\alpha^n - 1)(\beta^n - 1) = (\alpha\beta)^n - \alpha^n - \beta^n + 1 = (-1)^n - \alpha^n - \beta^n + 1^n$. Hence, we take
$g(x) = (x - \alpha)(x - \beta)(x - 1)(x + 1) = (x^2 + kx - 1)(x^2 - 1) = x^4 + kx^3 - 2x^2 - kx + 1$.
This gives $A_{n+4} = -kA_{n+3} + 2A_{n+2} + kA_{n+1} - A_n$. □

We now aim to determine conditions for a_n having primitive prime divisors. As before, we aim to create an upper bound on an a_n with no primitive prime divisors in terms of the radical of n, and a lower bound of a_n which increases exponentially. To achieve this, we begin by imitating the method of Lemma 6.28.

First we introduce a lemma to allow us to deal with the case that $\alpha\beta = -1$.

Lemma 6.38. *If $\alpha\beta = -1$ and m is odd, then $A_{2m} = -A_m^2$ and $|a_{2m}| = |a_m|$.*

Proof. We have

$$\begin{aligned} A_m &= (\alpha^m - 1)(\beta^m - 1) = 1 + (\alpha\beta)^m - \alpha^m - \beta^m = -\alpha^m - \beta^m. \\ A_{2m} &= (\alpha^{2m} - 1)(\beta^{2m} - 1) = (\alpha^m - 1)(\beta^m - 1)(\alpha^m + 1)(\beta^m + 1) \\ &= A_m(1 + (\alpha\beta)^m + \alpha^m + \beta^m) = A_m(\alpha^m + \beta^m) = -A_m^2. \end{aligned}$$

To show that $|a_{2m}| = |a_m|$ we use the relation

$$A_{2m} = \prod_{d|2m} a_d = \prod_{d|m} a_d a_{2d}$$

and use induction on the number of prime factors of m. □

In light of this lemma we shall make use of the condition that $(\alpha\beta)^m = 1$ in subsequent lemmas. This is equivalent to requiring that m is even if $\alpha\beta = -1$ and having no additional condition if $\alpha\beta = 1$.

Lemma 6.39. *If $(\alpha\beta)^m = 1$, and $k \geq 3$ is the largest power of 2 dividing A_m, then $k + 2$ is the largest power of 2 dividing A_{2m}.*

Proof. We have

$$A_m = (\alpha^m - 1)(\beta^m - 1) = (\alpha\beta)^m - \alpha^m - \beta^m + 1 = 2 - \alpha^m - \beta^m,$$

and so we have

$$\begin{aligned} A_{2m} &= (\alpha^{2m} - 1)(\beta^{2m} - 1) = (\alpha^m - 1)(\beta^m - 1)(\alpha^m + 1)(\beta^m + 1) \\ &= A_m(1 + \alpha^m + \beta^m + (\alpha\beta)^m) = A_m(2 + \alpha^m + \beta^m) = A_m(4 - A_m). \end{aligned}$$

The result immediately follows. □

Lemma 6.40. *If $(\alpha\beta)^m = 1$, and $k \geq 2$ is the largest power of 3 dividing A_m, then $k + 2$ is the largest power of 3 dividing A_{3m}.*

Proof. We use the identity $x^3 - y^3 = 3xy(x - y) + (x - y)^3$ in the following. We have

$$\begin{aligned} A_{3m} &= (\alpha^{3m} - 1)(\beta^{3m} - 1) \\ &= (3\alpha^m(\alpha^m - 1) + (\alpha^m - 1)^3)(3\beta^m(\beta^m - 1) + (\beta^m - 1)^3) \\ &= (\alpha^m - 1)(3\alpha^m + (\alpha^m - 1)^2)(\beta^m - 1)(3\beta^m + (\beta^m - 1)^2) \\ &= A_m(9(\alpha\beta)^m + 3\alpha^m(\beta^m - 1)^2 + 3\beta^m(\alpha^m - 1)^2 + (\alpha^m - 1)^2(\beta^m - 1)^2) \\ &= A_m(9 + 3(1 - \alpha^m)(\beta^m - 1) + 3(1 - \beta^m)(\alpha^m - 1) + A_m^2) \\ &= A_m(9 - 6A_m + A_m^2) = A_m(9 + A_m(A_m - 6)). \end{aligned}$$

The result immediately follows. □

Lemma 6.41. *If p is an odd prime then there exist $a_1, a_2, \ldots, a_s$ such that*

$$x^p - y^p = (x - y)^p + a_1xy(x - y)^{p-2} + a_2x^2y^2(x - y)^{p-4} + \cdots + a_sx^sy^s(x - y),$$

and such that $s = (p - 1)/2$; $p \mid a_i$ for each $1 \leq i \leq s$, and $a_s = p$.

Proof. It is clear that such an expansion exists. To show that $p \mid a_i$, consider the expansion in GF(p). As $x^p - y^p = (x - y)^p$ in GF(p) we have

$$a_1xy(x - y)^{p-2} + a_2x^2y^2(x - y)^{p-4} + \cdots + a_sx^sy^s(x - y) = 0.$$

Hence choosing $y = 1$, we see that for all $x \in \mathrm{GF}(p)$ the numbers $a_1, a_2, \ldots, a_s$ satisfy

$$a_1x(x - 1)^{p-2} + a_2x^2(x - 1)^{p-4} + \cdots + a_sx^s(x - 1) = 0.$$

Now let $f(x) = a_1x(x-1)^{p-2} + a_2x^2(x-1)^{p-4} + \cdots + a_sx^s(x-1)$. If the coefficients in $f(x)$ are non-zero then $f(x)$ is a degree $p-1$ polynomial in x with p distinct roots. This is a contradiction, so we must have $f(x) = 0$. Inspecting $f(x)$, we see that the coefficient of x^{p-1} is a_1, so we must have $a_1 = 0$. Given $a_1 = 0$, we see the coefficient of x^{p-2} is a_2, so we deduce $a_2 = 0$. Continuing in the same way we deduce that each $a_i = 0$ in GF(p), and hence $p \mid a_i$ for each $1 \leq i \leq s$.

To show that $a_s = p$, we first divide both sides of our equation to get

$$\frac{x^p - y^p}{x-y} = (x-y)^{p-1} + a_1xy(x-y)^{p-3} + a_2x^2y^2(x-y)^{p-5} + \cdots + a_sx^sy^s.$$

We now consider the expansion for $x = r+1$ and $y = 1$. This gives

$$\frac{x^p - y^p}{x-y} = \frac{(r+1)^p - 1}{r} = \frac{r^p + pr^{p-1} + \cdots + pr}{r} = r^{p-1} + pr^{p-2} + \cdots + p.$$

Therefore, considering the equation modulo r we have $a_s \equiv p \pmod{r}$ for all r. Therefore $a_s = p$. □

Lemma 6.42. *If $(\alpha\beta)^m = 1$, $p \geq 5$ is a prime dividing A_m, and k is the largest power of p dividing A_m, then $k+2$ is the largest power of p dividing A_{pm}.*

Proof. In the following let $A = (\alpha^m - 1)$ and $B = (\beta^m - 1)$. This gives us $AB = A_m$,

$$\alpha^m B = \alpha^m(\beta^m - 1)^2 = (1 - \alpha^m)(\beta^m - 1) = -A_m$$

and similarly $\beta^m A^2 = -A_m$. We have $A_{pm} = (\alpha^{pm} - 1)(\beta^{pm} - 1)$, hence using Lemma 6.41 with $x = \alpha^m$ and $y = 1$ we have

$$\begin{aligned}
&\alpha^{pm} - 1 \\
&= (\alpha^m - 1)^p + a_1\alpha^m(\alpha^m - 1)^{p-2} + a_2\alpha^{2m}(\alpha^m - 1)^{p-4} + \cdots + a_s\alpha^{sm}(\alpha^m - 1) \\
&= A^p + a_1\alpha^m A^{p-2} + a_2\alpha^{2m}A^{p-4} + \cdots + a_s\alpha^{sm}A \\
&= p\alpha^{sm}A + a_{s-1}\alpha^{(s-1)m}A^3 + \cdots + a_1\alpha^m A^{p-2} + A^p,
\end{aligned}$$

with $p \mid a_i$ for each a_i. We expand A_{pm} as follows

$$\begin{aligned}
A_{pm} &= (\alpha^{pm} - 1)(\beta^{pm} - 1) \\
&= (p\alpha^{sm}A + a_{s-1}\alpha^{(s-1)m}A^3 + \cdots + A^p)(p\beta^{sm}B + a_{s-1}\beta^{(s-1)m}B^3 + \cdots + B^p) \\
&= AB(p\alpha^{sm} + A^2(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3})) \\
&\qquad (p\beta^{sm} + B^2(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3})) \\
&= A_m(p^2(\alpha\beta)^{sm} + p\beta^{sm}A^2(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3})
\end{aligned}$$

$$
\begin{aligned}
&+ p\alpha^{sm}B^2(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3}) \\
&+ A^2B^2(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3})(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3})) \\
&= A_m(p^2 - p\beta^{(s-1)m}A_m(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3}) \\
&\quad - p\alpha^{(s-1)m}A_m(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3}) \\
&\quad + A_m^2(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3})(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3})) \\
&= A_m(p^2 - pA_m(\beta^{(s-1)m}(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3}) \\
&\quad \alpha^{(s-1)m}(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3})) \\
&\quad + A_m^2(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3})(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3})).
\end{aligned}
$$

We now define K and L by

$$
\begin{aligned}
K &= \beta^{(s-1)m}(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3}) + \alpha^{(s-1)m}(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3}), \\
L &= (a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3})(a_{s-1}\beta^{(s-1)m} + \cdots + B^{p-3}).
\end{aligned}
$$

Hence we have $A_{pm} = A_m(p^2 - pA_mK + A_m^2L)$. We note that K and L are symmetric polynomials in α and β and so are integers. Therefore, we aim to show that $p \mid K$ and $p \mid L$ to give the result. We have

$$
\begin{aligned}
&\beta^{(s-1)m}(a_{s-1}\alpha^{(s-1)m} + \cdots + A^{p-3}) \\
=&(a_{s-1}(\alpha\beta)^{(s-1)m} + a_{s-2}\beta^m(\alpha\beta)^{(s-2)m}A^2 + \cdots + \beta^{(s-1)m}A^{p-3}) \\
=&(a_{s-1} + \beta^mA^2(a_{s-2} + a_{s-3}\beta^mA^2 + \cdots + \beta^{(s-2)m}A^{p-5})) \\
=&(a_{s-1} - A_m(a_{s-2} + a_{s-3}\beta^mA^2 + \cdots + \beta^{(s-2)m}A^{p-5})).
\end{aligned}
$$

Hence $K = 2a_{s-1} - A_mg(\alpha, \beta)$ where $g(\alpha, \beta)$ is a symmetric function of α and β and so an integer. This shows that $p \mid K$.

Finally, we have

$$
\begin{aligned}
L &= (a_{s-1}\alpha^{(s-1)m} + a_{s-2}\alpha^{(s-2)m}A^2 + \cdots + A^{p-3}) \\
&\quad (a_{s-1}\beta^{(s-1)m} + a_{s-2}\beta^{(s-2)m}B^2 + \cdots + B^{p-3}) \\
&= (a_{s-1}\alpha^{(s-1)m} + A^2(a_{s-2}\alpha^{(s-2)m} + \cdots + A^{p-5})) \\
&\quad (a_{s-1}\beta^{(s-1)m} + B^2(a_{s-2}\beta^{(s-2)m} + \cdots + B^{p-5})) \\
&= (a_{s-1}\alpha^{(s-1)m} + A^2h(\alpha, \beta))(a_{s-1}\beta^{(s-1)m} + B^2h(\beta, \alpha)) \\
&= (a_{s-1}^2(\alpha\beta)^{(s-1)m} + a_{s-1}(\alpha^{(s-1)m}B^2h(\beta, \alpha) + \beta^{(s-1)m}A^2h(\alpha, \beta)) \\
&\quad + A^2B^2h(\alpha, \beta)h(\beta, \alpha)) \\
&= (a_{s-1}^2 + a_{s-1}C + A_m^2D).
\end{aligned}
$$

The expressions for C and D are symmetric polynomials in α and β, and so are integers. We have that $p \mid a_{s-1}$ and $p \mid A_m$, hence $p \mid L$. □

We are now in a position to give a bound on a_n with no primitive prime divisor.

Lemma 6.43. *If a_n has no primitive prime divisor, and $n \notin \{2, 3, 4, 6\}$, then $a_n \leq \mathrm{rad}(n)^2$.*

Proof. Suppose that a_n has no primitive prime divisors and $p \mid a_n$. As $p \mid a_n$ and p is not a primitive prime divisor we must have that $p \mid n$. We consider separately the cases $p = 2$, $p = 3$ and $p \notin \{2, 3\}$.

If $p \notin \{2, 3\}$ we can use Lemma 6.42. Letting $n = pm$ we have from $p \mid a_{pm}$ that $p \mid a_m$ and hence $p \mid A_m$. If m is odd and $\alpha\beta = -1$ then from Lemma 6.38 we may consider a_{2m} instead of a_m so that $(\alpha\beta)^{2m} = 1$, and use the fact $|a_{2m}| = |a_m|$ to deduce the factors of a_m, so we now suppose $(\alpha\beta)^m = 1$. Letting λ be defined such that $p^\lambda \mid\mid A_m$, from Lemma 6.42 we have that $p^{\lambda+2} \mid\mid A_{pm}$. Therefore, from $A_{pm} = \prod_{d \mid pm} a_d = A_m \prod_{d \mid m} a_{pd}$ we see that no power of p higher than p^2 can divide a_{pm}.

To deal with the case $p = 2$ we first consider point (v) of Lemma 6.35. This tells us that if $2 \mid a_n$ then $n = k2^r$ where k is the multiplicative order of a root of $f(x)$ in GF(2). There are two possibilities for the value of $f(x)$ in GF(2) which we consider separately. First, suppose that $f(x) = x^2 + 1$ in GF(2). In this case $f(x) = (x + 1)^2$ and has two roots of multiplicative order 1. Hence, $2 \mid a_n$ implies $n = 2^r$ for some $r \geq 1$. From Lemma 6.39 we know that if $2^3 \mid A_{2^c}$ then 2^2 is the highest possible power of 2 which can divide any a_{2^r} for $r > c$. We consider the sequence $\langle A_i \rangle$ modulo 2^3. We may do this using Lemma 6.37, noting that as the sequence is a linear recurrence it is periodic modulo any modulus; and that the sequence is determined by the value of k modulo 2^3 and the value of $\alpha\beta$. We now calculate the smallest n such that $2^3 \mid A_n$ and $n = 2^r$ for each possible value of $f(x) \pmod{2^3}$.

$f(x)$	Period	n
$x^2 + 1$	0, 2, 4, 2	4
$x^2 + 2x + 1$	0, 4	2
$x^2 + 4x + 1$	0, 6, 4, 6	4
$x^2 + 6x + 1$	0	1
$x^2 - 1$	0	1
$x^2 + 2x - 1$	0, 2, 4, 6	4
$x^2 + 4x - 1$	0, 4	2
$x^2 + 6x - 1$	0, 6, 4, 2	4

Hence for $n \notin \{1, 2, 4\}$ we find that 2^2 is the highest power of 2 which can divide a_n in these cases.

Now we consider the case $f(x) = x^2 + x + 1$ in GF(2). The roots of this polynomial have multiplicative order 3, so $2 \mid a_n$ implies $n = 3 \times 2^r$ for some $r \geq 0$. Again, we calculate the sequence $\langle A_i \rangle$ modulo 2^3 in order to find the smallest A_n such that $2^3 \mid A_n$ and $n = 3 \times 2^r$ so that we may apply Lemma 6.39. We calculate the smallest A_n with $2^3 \mid A_n$ and $n = 3 \times 2^r$ for each possible $f(x) \pmod{2^3}$ as follows.

$f(x)$	Period	n
$x^2 + x + 1$	0, 3, 3	3
$x^2 + 3x + 1$	0, 5, 3, 4, 3, 5	6
$x^2 + 5x + 1$	0, 7, 3, 0, 3, 7	3
$x^2 + 7x + 1$	0, 1, 3, 4, 3, 1	6
$x^2 + x - 1$	0, 1, 7, 4, 3, 3, 0, 5, 3, 4, 7, 7	6
$x^2 + 3x - 1$	0, 3, 7, 4, 3, 1, 0, 7, 3, 4, 7, 5	6
$x^2 + 5x - 1$	0, 5, 7, 4, 3, 7, 0, 1, 3, 4, 7, 3	6
$x^2 + 7x - 1$	0, 7, 7, 4, 3, 5, 0, 3, 3, 4, 7, 1	6

Hence for $n \notin \{3, 6\}$ we find that 2^2 is the highest power of 2 which can divide a_n in these cases.

We now treat the remaining cases for the prime $p = 3$ in the same way as for $p = 2$. We first consider the case where $f(x) = x^2 + 1$ in GF(3). In this case $f(x)$ has two roots of order 4, and so $3 \mid a_n$ implies $n = 4 \times 3^r$ for some $r \geq 0$. We now calculate $\langle A_i \rangle$ for each possible $f(x) \pmod{3^2}$ to find the first n such that $3^2 \mid A_n$ and $n = 4 \times 3^r$ as follows.

$f(x)$	Period	n
$x^2 + 1$	0, 2, 4, 2	4
$x^2 + 3x + 1$	0, 5, 4, 2, 0, 8, 4, 8, 0, 2, 4, 5	4
$x^2 + 6x + 1$	0, 8, 4, 2, 0, 5, 4, 5, 0, 2, 4, 8	4

Hence for $n \neq 4$ we find that 3^2 is the highest power of 3 which can divide a_n in these cases.

For the case $f(x) = x^2 - 1$ in GF(3) we have that $f(x)$ has roots of order 1 and 2. Therefore $3 \mid a_n$ implies $n = 3^r$ or $n = 2 \times 3^r$. We calculate the smallest n such that $3^2 \mid A_n$ for $n = 3^r$ and $n = 2 \times 3^r$ as follows.

$f(x)$	Period	n
$x^2 - 1$	0	1, 2
$x^2 + 3x - 1$	0, 3, 0, 0, 0, 6	2
$x^2 + 6x - 1$	0, 6, 0, 0, 0, 3	2

Hence for $n \neq 2$ we find that 3^2 is the highest power of 3 which can divide a_n in these cases.

For the case $f(x) = x^2 + x + 1$ in GF(3) we have that $f(x) = (x-1)^2$, so has two roots of order 1. Therefore if $3 \mid a_n$ we have that $n = 3^r$. For each $f(x) \mod 3^2$ we calculate the smallest n such that $3^2 \mid A_n$ and $n = 3^r$ as follows.

$f(x)$	Period	n
$x^2 + x + 1$	0, 3, 3	3
$x^2 + 4x + 1$	0, 6, 6	3
$x^2 + 7x + 1$	0	1

Hence for $n \notin \{1, 3\}$ we find that 3^2 is the highest power of 3 which can divide a_n in these cases.

For the cases $f(x) = x^2 + x - 1$ and $f(x) = x^2 + 2x - 1$ we have that $f(x)$ has two roots of order 8. Hence if $3 \mid a_n$ we have that $n = 8 \times 3^r$. For each $f(x) \pmod{3^2}$ we calculate the smallest n such that $3^2 \mid A_n$ and $n = 8 \times 3^r$ as follows.

$f(x)$	Period	n
$x^2 + x - 1$	0, 1, 8, 4, 4, 2, 2, 2, 0, 4, 5, 1, 4, 8, 5, 5, 0, 7, 2, 7, 4, 5, 8, 8	8
$x^2 + 4x - 1$	0, 4, 2, 4, 4, 5, 2, 5	8
$x^2 + 7x - 1$	0, 7, 5, 4, 4, 8, 2, 8, 0, 4, 8, 7, 4, 2, 8, 5, 0, 1, 2, 1, 4, 5, 5, 2	8
$x^2 + 2x - 1$	0, 2, 5, 5, 4, 1, 2, 1, 0, 5, 8, 2, 4, 7, 8, 4, 0, 8, 2, 8, 4, 4, 5, 7	8
$x^2 + 5x - 1$	0, 5, 2, 5, 4, 4, 2, 4	8
$x^2 + 8x - 1$	0, 8, 8, 5, 4, 7, 2, 7, 0, 5, 5, 8, 4, 1, 5, 4, 0, 2, 2, 2, 4, 4, 8, 1	8

Hence for $n \neq 8$ we find that 3^2 is the highest power of 3 which can divide a_n in these cases.

Finally, in the case $f(x) = x^2 + 2x + 1$ in GF(3) we have that $f(x) = (x-1)^2$ so has two roots of order 2. Hence if $3 \mid a_n$ we have that $n = 2 \times 3^r$. For each $f(x) \pmod{3^2}$ we calculate the smallest n such that $3^2 \mid A_n$ and $n = 2 \times 3^r$ as follows.

$f(x)$	Period	n
$x^2 + 2x + 1$	0, 4	2
$x^2 + 5x + 1$	0, 7, 6, 4, 6, 7	6
$x^2 + 8x + 1$	0, 1, 3, 4, 3, 1	6

Hence for $n \notin \{2, 6\}$ we find that 3^2 is the highest power of 3 which can divide a_n in these cases.

Finally, combining all of these special cases, we see that for $n \notin \{2, 3, 4, 6\}$ we have that if $p \mid a_n$ and $p \mid n$ then p^2 is the highest power of p which can divide a_n. □

We now aim to find a lower bound on a_n. We aim to create a bound independent of k, so we begin with lemmas relating the sequences $\langle a_n \rangle$ for different values of k. We begin by considering the case $\alpha\beta = -1$.

Lemma 6.44. *Letting $a_n = \Phi_n(\alpha)\Phi_n(\beta)$ and $b_n = \Phi_n(\gamma)\Phi_n(\delta)$ where α and β are the roots of $x^2 + kx - 1$ and γ and δ are the roots of $x^2 - kx - 1$ we have $a_n = b_n$ for $n > 2$.*

Proof. Without loss of generality we have $\gamma = -\alpha$ and $\delta = -\beta$. Hence, we have $\beta = -\alpha^{-1}$ and $\delta = -\gamma^{-1} = \alpha^{-1}$. For $n > 1$, the polynomial $\Phi_n(x)$ is symmetric, so $\Phi_n(x) = x^{\varphi(n)}\Phi_n(x^{-1})$. Altogether this gives

$$\begin{aligned} b_n &= \Phi_n(\gamma)\Phi_n(\delta) = \Phi_n(-\alpha)\Phi_n(\alpha^{-1}) = (-\alpha)^{\varphi(n)}\Phi_n(-\alpha^{-1})(\alpha^{-1})^{\varphi(n)}\Phi_n(\alpha) \\ &= (-\alpha\alpha^{-1})^{\varphi(n)}\Phi_n(\alpha)\Phi_n(-\alpha^{-1}) = (-1)^{\varphi(n)}\Phi_n(\alpha)\Phi_n(\beta) = a_n. \end{aligned}$$

We have $(-1)^{\varphi(n)} = 1$ as $\varphi(n)$ is even for $n > 2$. □

In light of this lemma, when $\alpha\beta = -1$ we shall only consider $k > 0$ when establishing a lower bound on a_n.

Lemma 6.45. *For $n > 2$, a_n is at a minimum when $k = 1$.*

Proof. Rearranging our expression for a_n we have

$$\begin{aligned} a_n &= \Phi_n(\alpha)\Phi_n(\beta) \\ &= \prod_{\xi \in \rho(\Phi_n)} (\alpha - \xi)(\beta = \xi) \\ &= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (\alpha - \xi)(\beta - \xi^{-1})(\beta - \xi)(\alpha - \xi^{-1}) \\ &= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (\alpha\beta - \alpha\xi^{-1} - \beta\xi + 1)(\alpha\beta - \alpha\xi - \beta\xi^{-1} + 1) \\ &= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (\alpha\xi^{-1} + \beta\xi)(\alpha\xi + \beta\xi^{-1}) \\ &= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (\alpha^2 + \beta^2 + \alpha\beta\xi^2 + \alpha\beta\xi^{-2}) \\ &= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} ((\alpha + \beta)^2 - 2\alpha\beta + \alpha\beta(\xi^2 + \xi^{-2})) \\ &= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (k^2 + 2 - (\xi^2 + \xi^{-2})). \end{aligned}$$

We have that $-2 \leq \xi^2 + \xi^{-2} \leq 2$ as ξ is a root of unity. Hence $2 - (\xi^2 + \xi^{-2}) \geq 0$ and

each term in our equation for a_n is positive and strictly increasing with k. Hence a_n is at a minimum when $k = 1$. □

We now consider the sequence $\langle a_n \rangle$ for $\alpha\beta = 1$. In this case, as we consider $f(x) = x^2 + kx + 1$ only when it has no cyclotomic divisors, we have that $|k| \geq 3$. The following table shows the cyclotomic factors of $f(x)$ for $-2 \leq k \leq 2$.

k	$f(x)$	Factorised
-2	$x^2 - 2x + 1$	$\Phi_1(x)^2$
-1	$x^2 - x + 1$	$\Phi_6(x)$
0	$x^2 + 1$	$\Phi_4(x)$
1	$x^2 + x + 1$	$\Phi_3(x)$
2	$x^2 + 2x + 1$	$\Phi_2(x)^2$

Lemma 6.46. *If $k > 0$, then a_n is at a minimum for $k = 3$. If $k < 0$, then a_n is at a minimum for $k = -3$.*

Proof. We rearrange our expression for a_n as follows

$$\begin{aligned}
a_n &= \Phi_n(\alpha)\Phi_n(\beta) \\
&= \prod_{\xi \in \rho(\Phi_n)} (\alpha - \xi)(\beta - \xi) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (\alpha - \xi)(\beta - \xi^{-1})(\beta - \xi)(\alpha - \xi^{-1}) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (\alpha\beta - \alpha\xi^{-1} - \beta\xi + 1)(\alpha\beta - \beta\xi^{-1} - \alpha\xi + 1) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (2 - (\alpha\xi^{-1} + \beta\xi))(2 - (\beta\xi^{-1} + \alpha\xi)) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (4 - 2(\alpha\xi + \beta\xi + \alpha\xi^{-1} + \beta\xi^{-1}) + (\alpha\xi^{-1} + \beta\xi)(\alpha\xi + \beta\xi^{-1})) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (4 - 2(\alpha + \beta)(\xi + \xi^{-1}) + (\alpha^2 + \beta^2 + \alpha\beta\xi^2 + \alpha\beta\xi^{-2})) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (4 - 2(\alpha + \beta)(\xi + \xi^{-1}) + (\alpha + \beta)^2 - 2\alpha\beta + \alpha\beta(\xi^2 + \xi^{-2})) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (k^2 + 2(\xi + \xi^{-1})k + 2 + (\xi^2 + \xi^{-2})) \\
&= \prod_{\xi, \xi^{-1} \in \rho(\Phi_n)} (k + (\xi + \xi^{-1}))^2.
\end{aligned}$$

As ξ is a root of unity, we have $-2 \leq \xi + \xi^{-1} \leq 2$, hence for $k \geq 3$ each term in the product is positive and strictly increasing in k, so for $k > 0$ we have that a_n takes a minimum when $k = 3$. For $k \leq 3$ each term in the product is negative and strictly

decreasing with k, so for $k < 0$ we have that $|a_n|$ takes a minimum for $k = -3$. Finally, from our formula for a_n we have that a_n is the product of squares of real numbers, and hence $a_n > 0$, which completes the proof of the result. □

Hence we aim to find lower bounds for the sequences $\langle a_n \rangle$ corresponding to $f(x) = x^2 + x - 1$, $f(x) = x^2 + 3x + 1$ and $f(x) = x^2 - 3x + 1$. The polynomials $f(x) = x^2 + 3x + 1$ and $f(x) = x^2 - 3x + 1$ both have roots α and β satisfying $|\alpha| > 1$ and $|\beta| < 1/2$, so we may apply Lemma 6.31 in these cases. However, the polynomial $f(x) = x^2 + x - 1$ has roots α and β satisfying $|\alpha| > 1$ and $1/2 < |\beta| < 1$, so we need to modify Lemma 6.31 for this case.

Lemma 6.47. *If α is the root of $f(x) = x^2 + x - 1$ satisfying $1/2 < |\alpha| < 1$, then we have $\Phi_n(\alpha) \geq 1/12$ and $\Phi_n(-\alpha) \geq 1/12$.*

Proof. In this case, we note that we have

$$|\alpha|^2 + |\alpha|^3 + |\alpha|^3 + \cdots = \frac{|\alpha|^2}{1 - |\alpha|} = 1,$$

so we may use the inequality $(1 - x)(1 - y) \geq 1 - x - y$ for $0 \leq x, y \leq 1$ to show that

$$(1-|\alpha|^3)(1-|\alpha|^4)(1-|\alpha|^5)\cdots \geq (1-|\alpha|^3-|\alpha|^4)(1-|\alpha|^5)\cdots \geq 1-|\alpha|^3-|\alpha|^4-|\alpha|^5-\ldots.$$

Hence, as before we have

$$\begin{aligned}
\Phi_n(\alpha) &= \prod_{d|n}(1 - \alpha^{n/d})^{\mu(d)} \\
&\geq \prod_{i=1}^{\infty}(1 - |\alpha|^i) \\
&= (1 - |\alpha|)(1 - |\alpha|^2)\prod_{i=3}^{\infty}(1 - |\alpha|^i) \\
&= (1 - |\alpha| - |\alpha|^2 + |\alpha|^3)(1 - |\alpha|^3 - |\alpha|^4 - \ldots) \\
&= |\alpha|^3\left(1 - \frac{|\alpha|^3}{1 - |\alpha|}\right) > \frac{1}{12}.
\end{aligned}$$

The same immediately follows for $\Phi_n(-\alpha)$ from the same argument. □

We may now give inequalities for the sequence $\langle a_n \rangle$ in each of our cases of interest.

Lemma 6.48. *With the given choices of the polynomial $f(x)$, the sequence a_n satisfies the following lower bounds for $n > 2$.*

$f(x)$	Lower Bound
x^2+x-1	$(1/144)(3/2)^{\varphi(n)}$
x^2+3x+1	$(4/25)(5/2)^{\varphi(n)}$
x^2-3x+1	$(4/25)(5/2)^{\varphi(n)}$

Proof. For the polynomial $f(x)=x^2+x-1$, let α and β be the roots of $f(x)$ such that $|\alpha|>1$ and $1/2<|\beta|<1$. From Lemma 6.47 we have $\Phi_n(\beta),\Phi_n(-\beta)\geq 1/12$. We rearrange as follows

$$a_n=\Phi_n(\alpha)\Phi_n(\beta)=\alpha^{\varphi(n)}\Phi_n(\alpha^{-1})\Phi_n(\beta)=\alpha^{\varphi(n)}\Phi_n(-\beta)\Phi_n(\beta)\geq(1/144)(3/2)^{\varphi(n)}.$$

For the polynomial $f(x)=x^2+3x+1$ let α and β be the roots of $f(x)$ such that $|\alpha|>1$ and $0<|\beta|<1/2$. From Lemma 6.31 we have $\Phi_n(\beta)\geq 1-|\beta|-|\beta|^2\geq 2/5$. We arrange as follows

$$a_n=\Phi_n(\alpha)\Phi_n(\beta)=\alpha^{\varphi(n)}\Phi_n(\alpha^{-1})\Phi_n(\beta)=\alpha^{\varphi(n)}\Phi_n(\beta)^2\geq(4/25)(5/2)^{\varphi(n)}.$$

Finally, it can be seen that the same bound that applies to $f(x)=x^2+3x+1$ also applies to $f(x)=x^2-3x+1$. □

We now use these bounds to calculate which a_n have primitive prime divisors for each $f(x)$. We begin with the case $f(x)=x^2+kx-1$.

Proposition 6.49. *For $f(x)=x^2+kx-1$ and $n\notin\{1,2,3,4,6\}$ the number a_n has at least one primitive prime divisor unless $|k|=1$ and $n\in\{12,20,24\}$.*

Proof. We begin by considering $f(x)=x^2+x-1$, noting Lemma 6.45. By combining Lemma 6.43 and Lemma 6.48 we have that if $(1/144)(3/2)^{\varphi(n)}>\operatorname{rad}(n)^2$ then a_n has a primitive prime divisor. As in Lemma 6.33 we may use the inequality $x^{k-1}\geq k^2y$ for $x\geq y\geq 9$ and $k\geq 3$ to show that if $(3/2)^{\varphi(a)}\geq 576\operatorname{rad}(a)^2$ then $(3/2)^{\varphi(ap^e)}\geq 576\operatorname{rad}(ap^e)$ for any prime power p^e where $p\neq 2$.

Now suppose that there is some p^e such that $p^e\mid n$ and $(3/2)^{\varphi(p^e)}>576p^2$. Let $n=p^ep_1^{e_1}p_2^{e_2}\dots p_k^{e_k}q$ be a factorisation of n such that $p_i\notin\{2,p\}$, $p_i\neq p_j$ and q is a power of 2. As $(3/2)^{\varphi(p^e)}>576p^2$ we have $(3/2)^{\varphi(p^ep_1^{e_1}p_2^{e_2}\dots p_k^{e_k})}>576p^2p_1^2p_2^2\dots p_k^2$. Hence we have

$$\begin{aligned}(1/144)(3/2)^{\varphi(n)}&=(1/144)((3/2)^{\varphi(p^ep_1^{e_1}p_2^{e_2}\dots p_k^{e_k})})^{\varphi(q)}\\&>(1/144)(576p^2p_1^2p_2^2\dots p_k^2)^{\varphi(q)}\end{aligned}$$

$$\geq (1/144)(576p^2p_1^2p_2^2\dots p_k^2)$$
$$= 2^2p^2p_1^2p_2^2\dots p_k^2 \geq \mathrm{rad}(n)^2.$$

For any prime $p \geq 37$ we have $(3/2)^{\varphi(p)} \geq 576p^2$, so if n has a prime factor $p \geq 37$ we have that a_n has a primitive prime divisor. For any prime $p \geq 7$ we have $(3/2)^{\varphi(p^2)} \geq 576p^2$, so if n has a prime factor $p \geq 7$ such that $p^2 \mid n$ we have that a_n has a primitive prime divisor. For any prime $p \geq 5$ we have that $(3/2)^{\varphi(p^3)} \geq 576p^2$, hence if n has a prime factor $p \geq 5$ such that $p^3 \mid n$ we have that a_n has a primitive prime divisor. For any prime $p \geq 3$ we have that $(3/2)^{\varphi(p^4)} \geq 576p^2$, so if n has a prime factor $p \geq 3$ such that $p^4 \mid n$ we have that a_n has a primitive prime divisor. Finally, we have $(1/144)(3/2)^{\varphi(2^5)} \geq 2^2$, hence if n is a power of 2 such that $n \geq 2^5$ then a_n has a primitive prime divisor.

Altogether, we have shown that if $n \notin \{1, 2, 3, 4, 6\}$ is not of the form

$$n = 2^a3^b5^c7^d11^e13^f17^g19^h23^i29^j31^k$$

where $0 \leq a \leq 4$, $0 \leq b \leq 3$, $0 \leq c \leq 2$ and $0 \leq d, e, f, g, h, i, j, k \leq 1$ then a_n has a primitive prime divisor. By computer search, we find that this inequality holds for

$$n \notin \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25,$$
$$26, 27, 28, 29, 30, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 50, 52, 54, 56, 58,$$
$$60, 66, 70, 72, 78, 84, 90\}.$$

We may further reduce the size of this set by calculating a_n explicitly for each n in the set. This shows that for

$$n \notin \{1, 2, 3, 5, 6, 7, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30, 42\}$$

we have $a_n > \mathrm{rad}(n)^2$. Further, for $f(x) = x^2 + 2x - 1$ we reduce this set to $\{2, 3, 6, 10, 12\}$ and for $f(x) = x^2 + 3x - 1$ to $\{2, 6\}$. For $f(x) = x^2 + 2x - 1$ we have $a_{10} = 41$ and $a_{12} = 5^2$, so we have the result for $f(x) = x^2 + kx - 1$ where $|k| \neq 1$.

Finally, we manually calculate a_n for the special cases of n identified in the case $|k| = 1$ and determine when they have primitive prime factors. We have

$a_1 = 1$	$a_2 = -1$	$a_3 = 4$	$a_5 = 11$	$a_6 = 4$
$a_7 = 29$	$a_{10} = 11$	$a_{12} = 4$	$a_{14} = 29$	$a_{15} = 31$
$a_{18} = 19$	$a_{20} = 25$	$a_{21} = 211$	$a_{22} = 199$	$a_{24} = 36$
$a_{26} = 521$	$a_{28} = 169$	$a_{30} = 31$	$a_{42} = 211$	

and hence a_n has primitive prime divisors except for the cases
$n \in \{1, 2, 6, 12, 20, 24\}$. □

Proposition 6.50. *For $f(x) = x^2 + kx + 1$ where $|k| \geq 3$ we have that a_n has at least one primitive prime divisor for all $n \notin \{1, 2, 3, 4, 6\}$ unless $k = 3$ and $n \in \{5, 12\}$ or $k = -3$ and $n = 12$.*

Proof. We begin by considering $f(x) = x^2 \pm 3x + 1$ noting Lemma 6.46 and the fact the inequalities for $f(x) = x^2 + 3x + 1$ and $f(x) = x^2 - 3x + 1$ are the same in Lemma 6.48. By combining Lemma 6.43 and Lemma 6.48 we have that if $(4/25)(5/2)^{\varphi(n)} > \operatorname{rad}(n)^2$ and $n \notin \{1, 2, 3, 4, 6\}$ then a_n has a primitive prime divisor. As in Lemma 6.33, from the inequality $x^{k-1} \geq k^2 y$ for $x \geq y \geq 9$ and $k \geq 3$ we may show that if $(5/2)^{\varphi(a)} \geq 25 \operatorname{rad}(a)^2$ then $(5/2)^{\varphi(ap^e)} \geq 25 \operatorname{rad}(ap^e)^2$ for any prime power p^e where $p \neq 2$.

Now suppose that there exists some prime power p^e such that $p^e \mid n$ and $(5/2)^{\varphi(p^e)} > 25p^2$. Let $n = p^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} q$ be a prime factorisation of n where $p_i \notin \{p, 2\}$, $p_i \neq p_j$ and q is a power of 2. As $(5/2)^{\varphi(p^e)} > 25p^2$ we have $(5/2)^{\varphi(p^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k})} > 25p^2 p_1^2 p_2^2 \dots p_k^2$. Hence we have

$$\begin{aligned}
(4/25)(5/2)^{\varphi(n)} &= (4/25)((5/2)^{\varphi(p^e p_1^{e_1} p_2^{e_2} \dots p_k^{e_k})})^{\varphi(q)} \\
&> (4/25)(25p^2 p_1^2 p_2^2 \dots p_k^2)^{\varphi(q)} \\
&\geq (4/25)(25p^2 p_1^2 p_2^2 \dots p_k^2) \\
&= 2^2 p^2 p_1^2 p_2^2 \dots p_k^2 \geq \operatorname{rad}(n)^2.
\end{aligned}$$

For all $p \geq 11$ we have $(5/2)^{\varphi(p)} \geq 25p^2$, hence if $p \geq 11$ and $p \mid n$ we have that a_n has at least one primitive prime divisor. For $p \geq 3$ we have that $(5/2)^{\varphi(p^2)} \geq 25p^2$, hence if $p \geq 3$ and $p^2 \mid n$ we have that a_n has at least one primitive prime divisor. Finally, for $p \geq 2$ we have that $(5/2)^{\varphi(p^4)} \geq 25p^2$, hence if $p \geq 2$ and $p^4 \mid n$ we have that a_n has at least one primitive prime divisor. If a_n does not have a primitive prime divisor we must have

$$n = 2^a 3^b 5^c 7^d$$

for some $0 \leq a \leq 3$ and $0 \leq b, c, d \leq 1$. Further, by manually checking the inequality we find that $(4/25)(5/2)^{\varphi(n)} > \operatorname{rad}(n)^2$ holds for all cases except $n \in \{1, 2, 3, 4, 5, 6, 7, 10, 12, 14, 30\}$. Calculating a_n explicitly in these cases shows that

we have $a_n \leq \mathrm{rad}(n)^2$ only in the cases $n \in \{2, 3, 5, 6, 12\}$. Further, for $|k| = 4$ this set becomes $\{2, 3, 6\}$, so the result follows for $|k| \geq 4$. Finally, calculating a_n for $n = 5$ and $n = 12$ in the case $k = 3$ we have $a_5 = 25$ and $a_{12} = 36$, and neither has a primitive prime divisor. In the case $k = -3$ we have $a_5 = 121$ and $a_{12} = 36$, and hence a_5 has a primitive prime divisor and a_{12} does not. □

Hence we have the result for $f(x) = x^2 + 4x + 1$ there is at least one primitive prime divisor of a_n for all n except $n \in \{1, 2, 3, 4, 6\}$. Further, by explicit calculation we have

$$a_1 = 6, \quad a_2 = -2, \quad a_3 = 9, \quad a_4 = 16 \quad \text{and} \quad a_6 = 25.$$

Hence, for $f(x) = x^2 + 4x + 1$, a_n has at least one primitive prime divisor if, and only if, $n \notin \{1, 2, 3, 4\}$. Therefore we have the following proposition.

Proposition 6.51. *There is a hyperbolic $(6, 6, m)$-regular map whose automorphism group is a fractional linear group for all $m \geq 5$.*

Proof. At the beginning of this section we showed that there exists a $(6, 6, m)$-regular map with automorphism group a fractional linear group over a finite field of characteristic p if, and only if, there exists a root of $x^2 + 4x + 1 = 0$ in some extension of $\mathrm{GF}(p)$ of order m. From Proposition 6.50 we have that there exist primes for all $m \notin \{1, 2, 3, 4, 6\}$ such that $x^2 + 4x + 1 = 0$ has a root of order m in some finite field. □

We have also been careful to state our work as generally as we can throughout this section as we are in a position to prove properties of Fibonacci like sequences. The sequences corresponding to $f(x) = x^2 - kx - 1$ are called *k-Fibonacci sequences* and some existing results concerning their periods may be found in [27]. For $f(x) = x^2 + kx \pm 1$ with roots α and β, define the sequence $\langle u_n \rangle$ by $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, or equivalently by $u_0 = 0$, $u_1 = 1$ and $u_{n+2} = -ku_{n+1} \mp u_n$. We define the *period* of $\langle u_n \rangle$ modulo a prime p to be the smallest $m > 0$ such that $u_i \equiv u_{i+m} \pmod{p}$ for all i. We denote by $\pi(p)$ the period of $\langle u_n \rangle$ modulo p. We now give our result concerning periods of these sequences.

Proposition 6.52. *For $f(x) = x^2 + kx + 1$, there exists some prime p for any $m \notin \{1, 2, 3, 4, 5, 6, 12\}$ such that $\pi(p) = m$.*

Proof. The sequence associated with the polynomial $f(x) = x^2 + kx + 1$ is $\langle u_n \rangle$ where $u_0 = 0$, $u_1 = 1$ and $u_{n+2} = -ku_{n+1} - u_n$. We have that the sequence $\langle x^n \rangle$ in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ is given by $x^n = u_n x + u_{n-1}$. Hence the order of x in

$(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ is equal to the period of $\langle u_n\rangle$ modulo p, i.e. $\text{ord}(x) = \pi(p)$. We now consider three cases of reducibility of $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

If $f(x)$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$, then $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle \cong \text{GF}(p^2)$ by an isomorphism ϕ where $\phi(x)$ is a root α of $f(x)$ in $\text{GF}(p^2)$. Hence the order of x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ is equal to the multiplicative order of α. Further, if the roots of $f(x)$ are α and β we have $\text{ord}(\alpha) = \text{ord}(\beta)$ from the fact $\alpha\beta = 1$.

If $f(x)$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ and has two roots α and β such that $\alpha \neq \beta$, then by the Chinese remainder theorem we have

$$(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\alpha\rangle \oplus (\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\beta\rangle.$$

Hence the order of x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ is the same as the least common multiples of the orders of x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\alpha\rangle$ and x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle x-\beta\rangle$, i.e. α and β in $\text{GF}(p)$. Again, we have $\text{ord}(\alpha) = \text{ord}(\beta)$ as $\alpha\beta = 1$, and so $\pi(p) = \text{ord}(\alpha)$.

If $f(x)$ is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ then $f(x)$ has a repeated root α in $\text{GF}(p)$. In this case, if $p \mid a_n$ then n is of the form $n = mp^r$ where m is the multiplicative order of α in $\text{GF}(p)$. As $f(x)$ has a repeated root in $\text{GF}(p)$, we must have that the discriminant of $f(x)$, Δ_f, is zero in $\text{GF}(p)$. We have $\Delta_f = k^2 - 4$, therefore we must have $p \mid k^2 - 4 = (k-2)(k+2)$. If α and β are the roots of $f(x)$ in $\mathbb{C}$, we have $\alpha + \beta = -k$ and $\alpha\beta = 1$, and so

$$a_1 = \Phi_1(\alpha)\Phi_2(\beta) = (\alpha-1)(\beta-1) = \alpha\beta - \alpha - \beta + 1 = 2 + k,$$

$$a_2 = \Phi_2(\alpha)\Phi_2(\beta) = (\alpha+1)(\beta+1) = \alpha\beta + \alpha + \beta + 1 = 2 - k.$$

Hence, in $\text{GF}(p)$ where $f(x) = (x-\alpha)^2$ we have $\text{ord}(\alpha) \in \{1, 2\}$.

Finally, we may apply Proposition 6.50 and note that for all $n \notin \{1, 2, 3, 4, 5, 6, 12\}$ there exists some prime p such that $p \mid a_n$ is a primitive prime divisor of a_n, and so there exists some $\alpha \in \text{GF}(p)$ such that α is a root of $f(x)$, $\text{ord}(\alpha) = n$ and so $\pi(p) = n$. □

Proposition 6.53. *For $f(x) = x^2 + kx - 1$, there exists some prime p for any $m \notin \{1, 2, 3, 4, 6\}$ such that $\pi(p) = 2m$.*

Proof. For an arbitrary prime p we consider $f(x)$ in an extension of $\text{GF}(p)$ where $f(x)$ splits. Let α and $-\alpha^{-1}$ be the roots of $f(x)$ chosen so that $\text{ord}(\alpha) \leq \text{ord}(-\alpha^{-1})$. We have $(-\alpha^{-1})^n = (-1)^n\alpha^{-n}$. Hence, if $n = \text{ord}(\alpha)$ and $\text{ord}(\alpha)$ is even we have $(-\alpha^{-1})^n = 1$, and so $\text{ord}(-\alpha^{-1}) = n$ as $\text{ord}(-\alpha^{-1}) \geq n$. Otherwise, if $n = \text{ord}(\alpha)$ and

$\mathrm{ord}(\alpha)$ is odd we have $(-\alpha^{-1})^n = -1$ so $\mathrm{ord}(-\alpha^{-1}) = 2n$. Therefore $f(x)$ either has all roots with the same even order, or one root with an odd order n and the other root with order $2n$.

The sequence $\langle u_n \rangle$ we consider is defined by $u_0 = 0$, $u_1 = 1$ and $u_{n+2} = -ku_{n+1} + u_n$. Again, we have that the period of this sequence modulo p is equal to the order of x in the ring $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$. We now consider three cases depending on whether $f(x)$ is irreducible in $\mathrm{GF}(p)$, has distinct roots in $\mathrm{GF}(p)$ or has a repeated root in $\mathrm{GF}(p)$.

If $f(x)$ is irreducible in $\mathrm{GF}(p)$ then $f(x)$ has two roots α and β in $\mathrm{GF}(p^2)$ and there exists an automorphism $\phi : \mathrm{GF}(p^2) \to \mathrm{GF}(p^2)$ such that $\phi(\alpha) = \beta$. Hence we have $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$, and so the order of α is some even number n, and p is a primitive prime divisor of a_n. Further, we have that $\mathrm{GF}(p^2) \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$, so $\mathrm{ord}(x) = \mathrm{ord}(\alpha)$ where $\mathrm{ord}(x)$ is the multiplicative order of x in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$. This gives $\pi(p) = \mathrm{ord}(x) = \mathrm{ord}(\alpha)$.

If $f(x)$ is reducible in $\mathrm{GF}(p)$ and has distinct roots α and β then either we have $\mathrm{ord}(\alpha) = \mathrm{ord}(\beta)$ and $\mathrm{ord}(\alpha)$ and $\mathrm{ord}(\beta)$ are even or we have, without loss of generality, $\mathrm{ord}(\alpha) = 2\,\mathrm{ord}(\beta)$. In either case, there exists one n such that n is even and p is a primitive prime divisor of a_n. Further, from the Chinese remainder theorem we have that

$$(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle x - \alpha \rangle \oplus (\mathbb{Z}/p\mathbb{Z})[x]/\langle x - \beta \rangle \cong \mathbb{Z}/p\mathbb{Z} \circ \mathbb{Z}/p\mathbb{Z},$$

by an isomorphism ϕ satisfying $\phi(x) = (\alpha, \beta)$, so $\mathrm{ord}(x) = (\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$. In either case we have $(\mathrm{ord}(\alpha), \mathrm{ord}(\beta)) = \mathrm{ord}(\alpha)$, hence we have $\mathrm{ord}(x) = \mathrm{ord}(\alpha)$, so $\pi(p) = \mathrm{ord}(\alpha)$. Therefore we have $\pi(p) = n$ where n is even and p is a primitive prime divisor of n.

If $f(x)$ is reducible in $\mathrm{GF}(p)$ and $f(x)$ has a repeated root α, then we have that the discriminant Δ_f of $f(x)$ is 0 in $\mathrm{GF}(p)$. We have $\Delta_f = k^2 + 4$, hence we must have $p \mid k^2 + 4$. We also have

$$a_4 = \Phi_4(\alpha)\Phi_4(\beta) = (\alpha^2{+}1)(\beta^2{+}1) = (\alpha\beta)^2{+}\alpha^2{+}\beta^2{+}1 = 2{+}(\alpha{+}\beta)^2{-}2\alpha\beta = k^2{+}4.$$

As α is a repeated root of $f(x)$ in $\mathrm{GF}(p)$ there is only one n such that p is a primitive prime divisor of a_n, and hence for odd p this is a_4. Otherwise, if $p = 2$ we have that p is a primitive prime divisor of a_1 due to the fact $2 \mid a_4 = a_{1\times 2^2}$ implies $2 \mid a_1$.

Hence, we see that for all primes p, letting $n = \pi(p)$ we either have p is a primitive prime divisor of a_1 or a_4 and no other a_k, or we have p is a primitive prime divisor of

a_n and possibly $a_{n/2}$ and no other a_k. Hence, if n is even and p is a primitive prime divisor of a_n where $n \geq 4$ we have $\pi(p) = n$. □

6.4 General Case

We now move onto consideration of the general case. We now wish to determine for which $k, l, m \in \mathbb{N}$ there exist solutions to the equation

$$\omega_k + \omega_l + \omega_m + 2 = 0$$

in some finite field. We begin by defining $N(k, l, m)$ as follows

$$N(k, l, m) = \prod(\omega_k + \omega_l + \omega_m + 2)$$

where the product is taken over as ω_k, ω_l and ω_m range over the roots of Ψ_k, Ψ_l and Ψ_m respectively.

Lemma 6.54. *$N(k, l, m) \in \mathbb{Z}$.*

Proof. We have that $N(k, l, m)$ is a symmetric function in the roots of polynomials whose coefficients lie in $\mathbb{Z}$, therefore $N(k, l, m) \in \mathbb{Z}$. □

Lemma 6.55. *There is a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ in a finite field of characteristic p if, and only if, $p \mid N(k, l, m)$.*

Proof. Considering the expression of $N(k, l, m)$ in an algebraically closed field of characteristic p, say K, we see that $N(k, l, m) = 0$ if, and only if, there is a solution to $\omega_k + \omega_l + \omega_m + 2 = 0$ in K for ω_k, ω_l and ω_m roots of Ψ_k, Ψ_l and Ψ_m respectively. Further, as $N(k, l, m) \in \mathbb{Z}$ we have that $N(k, l, m) = 0$ in K if, and only if, $p \mid N(k, l, m)$. □

We now define the polynomials $f_{k,l}(x) \in \mathbb{Z}[x]$ and show that the condition $p \mid N(k, l, m)$ is equivalent to $f_{k,l}(x)$ having a root of multiplicative order m in a finite field of characteristic p. We define $f_{k,l}(x)$ as follows

$$f_{k,l}(x) = \prod \left(x^2 + (\omega_k + \omega_l + 2)x + 1\right)$$

where the product is taken as ω_k and ω_l range over the roots of Ψ_k and Ψ_l respectively.

Lemma 6.56. *A prime $p \nmid k, l, m$ is a divisor of $N(k, l, m)$ if, and only if, $f_{k,l}(x)$ has a root of order m in an extension of* GF(p).

Proof. Suppose that $N(k, l, m) = 0$ in GF(p), then in a suitable extension of GF(p) we have

$$\begin{aligned} N(k,l,m) &= \prod(\omega_k + \omega_l + \omega_m + 2) \\ &= \prod \xi_m^{-1}(\xi_m^2 + (\omega_k + \omega_l + 2)\xi_m + 1) = \alpha \prod f_{k,l}(\xi_m), \end{aligned}$$

where α is the product of m^{th} roots of unity and thus non-zero. Hence the product $\prod f_{k,l}(\xi_m)$ taken over the m^{th} roots of unity must have at least one term equal to zero, which is equivalent to $f_{k,l}(x)$ having a root of order m in an extension of GF(p).

For the converse, suppose that ξ_m is a root of $f_{k,l}(x)$ in an extension of GF(p). We have

$$0 = f_{k,l}(\xi_m) = \prod(\xi_m^2 + (\omega_k + \omega_l + 2)\xi_m + 1),$$

so there is some ω_k and ω_l from the product where we have $\xi_m^2 + (\omega_k + \omega_l + 2)\xi_m + 1 = 0$. This gives

$$0 = \xi_m^2 + (\omega_k + \omega_l + 2)\xi_m + 1 = \xi_m(\omega_k + \omega_l + \omega_m + 2).$$

Hence, as $\xi_m \neq 0$, we must have $\omega_k + \omega_l + \omega_m + 2 = 0$. □

In light of this lemma we shall now aim to prove the following result. The author is unfamiliar with this result in the literature. However, there is a version (albeit with minor errors) available in a forum post here [48]. We use the method suggested from this post, correct the errors and develop the result further to give a constructive method.

Proposition 6.57. *For any monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $x \nmid f(x)$ and $\Phi_n(x) \nmid f(x)$ for all n there are only finitely many $m \in \mathbb{N}$ such that $f(x)$ has no root of order m in any finite field.*

Applying this to each polynomial $f_{k,l}(x)$ will allow us to determine that there are only finitely many m such that $f_{k,l}(x)$ has no root of order m in any finite field; there are only finitely many m for which

$$\omega_k + \omega_l + \omega_m + 2 = 0$$

has no solution in any finite field; and therefore that there are only finitely many m such that there is no (k, l, m)-regular map with automorphism group some fractional linear group. First, however, we must show that each $f_{k,l}(x)$ has at least one factor satisfying the conditions of Proposition 6.57.

Lemma 6.58. *If $k, l \in \mathbb{Z}$ is a hyperbolic pair then the polynomial $f_{k,l}(x)$ has at least one factor $g(x) \in \mathbb{Z}[x]$ such that $x \nmid g(x)$ and $\Phi_n \nmid g(x)$ for any n.*

Proof. From our definition of $f_{k,l}(x)$ we have

$$f_{k,l}(x) = \prod (x^2 + (\omega_k + \omega_l + 2)x + 1)$$

where the product is taken as ω_k and ω_l range over the roots of Ψ_k and Ψ_l respectively. Clearly we see that $x \nmid f_{k,l}(x)$ and thus $x \nmid g(x)$ for any factor $g(x)$ of $f_{k,l}(x)$. An expression of the form $x^2 + Cx + 1$ has two real roots, neither of which have absolute value 1, provided that $C^2 - 4 > 0$. Therefore, if there is some ω_k and ω_l such that $(\omega_k + \omega_l + 2)^2 > 4$ then $f_{k,l}(x)$ has real roots of absolute value not equal to 1, and therefore has at least one irreducible factor $g(x)$ such that $\Phi_n(x) \nmid g(x)$ for any n. We now consider different values of k and l.

For $n \geq 5$, taking $\xi = e^{i2\pi/n}$ we have that ξ is an n^{th} root of unity and that $\omega = \xi + \xi^{-1} = 2\cos(2\pi/n) > 0$. Hence if $k, l \geq 5$ we may find some $\omega_k, \omega_l > 0$ giving $(\omega_k + \omega_l + 2)^2 > 4$ as required.

For $k = 4$ we have $\omega_k = 0$, so for $l \geq 5$ we may find some $\omega_l > 0$ so a pair such that $(\omega_k + \omega_l + 2)^2 > 4$.

For $k = 3$ we have $\omega_k = -1$, so for $l \geq 7$ taking $\xi_l = e^{i2\pi/l}$ we have $\omega_l = \xi_l + \xi_l^{-1} = 2\cos(2\pi/l) > 1$. Thus we have $(\omega_k + \omega_l + 2)^2 > 4$.

Clearly the cases in which $l = 3$ or $l = 4$ are symmetric to those in which $k = 3$ or $k = 4$.

Hence for all parameters $k, l \in \mathbb{N}$ such that $1/k + 1/l > 1/2$ (i.e. k and l is a hyperbolic pair) we have that $f_{k,l}(x)$ has at least one root of absolute value not equal to 1, and thus there is a factor $g(x)$ of $f_{k,l}(x)$ satisfying the desired properties. □

We now prove Proposition 6.57. For the remainder of this section, let $f(x) \in \mathbb{Z}$ be a monic irreducible polynomial such that $f(x) \neq x$ and $f(x) \neq \Phi_n(x)$ for any n. Similarly to the previous section, we consider the sequences $\langle A_n \rangle$ and $\langle a_n \rangle$ defined as

follows

$$A_n = \prod_{\alpha \in \rho(f)} (\alpha^n - 1) \quad \text{and} \quad a_n = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha).$$

We first show the following properties of the sequences $\langle A_n \rangle$ and $\langle a_n \rangle$. Note in the following we denote the *resultant* of the polynomials $f, g \in \mathbb{Z}[x]$ as $\mathrm{Res}(f, g)$.

Lemma 6.59. *The sequences $\langle A_n \rangle$ and $\langle a_n \rangle$ satisfy the following properties.*

i) $A_n, a_n \in \mathbb{Z}$ *for all* $n \geq 0$*;*

ii) $A_n = \prod_{d|n} a_d$*;*

iii) there is a root of $f(x)$ of order n in a finite field of characteristic p if, and only if, $p \nmid n$ and $p \mid a_n$;

iv) if $p \mid a_{pn}$ then $p \mid a_n$;

v) for each p there exists between one and $\deg(f)$ numbers k such that $p \mid a_{kp^r}$ for all $r \geq 0$ and $p \nmid a_n$ for all other n;

vi) there exist numbers $c_0, c_1, \ldots, c_{k-1}$ where $k = 2^{\deg(f)}$ such that $A_{n+k} = \sum_{i=0}^{k-1} c_i A_{n+i}$;

vii) $a_n = \mathrm{Res}(f, \Phi_n)$.

Proof. Properties (i), (ii), (iii), (iv), (v) and (vi) are analogous to the same properties in Lemma 6.35. Property (vii) follows from the rearrangement

$$\mathrm{Res}(f, g) = \prod_{\substack{\alpha \in \rho(f) \\ \beta \in \rho(g)}} (\alpha - \beta) = \prod_{\alpha \in \rho(f)} g(\alpha). \qquad \square$$

Based on these properties, as before we make the definition that p is a *primitive prime divisor* of a_n if $p \mid a_n$ and $p \nmid n$. Again, we have that p is a primitive prime divisor of a_n if, and only if, $f(x)$ has a root of order n in a finite field of character p.

We shall begin by determining a lower bound on the terms in the sequence $\langle a_n \rangle$ which do not have primitive prime divisors. First we shall require the following lemma, recalling the definition of the Mahler measure from the introduction.

Lemma 6.60. *The Mahler measure $\mathrm{M}(f)$ of f satisfies $\mathrm{M}(f) > 1$.*

Proof. From our assumptions we have $f(x) \neq x$ and $f(x) \neq \Phi_n(x)$ for any n. The definition of the Mahler measure of $f(x)$ is

$$\mathrm{M}(f) = \prod_{\substack{\alpha \in \rho(f) \\ |\alpha| \geq 1}} |\alpha|.$$

Hence we have $\mathrm{M}(f) \geq 1$ by definition. As $f(x)$ is monic we have $f(x) = \prod_{\alpha \in \rho(f)}(x - \alpha)$, so $c = \prod_{\alpha \in \rho(f)} \alpha \in \mathbb{Z}$. As $f(x) \neq x$ we must have $c \neq 0$. Suppose there is no $\alpha \in \rho(f)$ such that $|\alpha| > 1$. If there is some $\alpha \in \rho(f)$ such that $|\alpha| < 1$ then $\prod_{\alpha \in \rho(f)} |\alpha| < 1$, contradicting $\prod_{\alpha \in \rho(f)} \alpha \in \mathbb{Z}$. Hence, we must have $|\alpha| = 1$ for all $\alpha \in \rho(f)$. From this we can deduce that the r^{th} coefficient of $f(x)$ is no greater than $\binom{n}{r}$ where $n = \deg(f)$, so is one of only finitely many polynomials of degree n whose roots all have absolute value 1. Now let $\alpha \in \rho(f)$ be an arbitrary root of $f(x)$. Consider the powers α^k of α. If all of these powers are distinct, then there are infinitely many algebraic numbers of degree n and absolute value 1, contradicting that there are only finitely many polynomials of degree n whose roots are all absolute value 1. Therefore, the powers α^k of α are not all distinct, so α is a root of unity, but this contradicts that $f(x) \neq \Phi_n(x)$ for any n. Therefore, $f(x)$ must have at least one root α satisfying $|\alpha| > 1$, so $\mathrm{M}(f) > 1$. □

In the next lemma we shall require the use of Baker's theorem shown and developed by Baker in the classic papers [3, 4] and [5]. We shall use the following direct corollary of Baker's theorem.

Theorem 6.61. *If α is an algebraic number other than a root of unity, then there exists constants k and N depending only on α such that $|\alpha^n - 1| > n^{-k}$ for all $n > N$.*

We now give a lower bound on the terms a_n. We note that although the constants involved are effectively computable, the proof is for all practical intents and purposes non-constructive.

Lemma 6.62. *There are constants C and N such that $|a_n| > e^{C\sqrt{n}}$ for all $n > N$.*

Proof. We first find upper and lower bounds on the terms $\log(|A_n|)$. For each root α of $f(x)$ we give upper and lower bounds of $|\alpha^n - 1|$ for each of the cases $|\alpha| < 1$, $|\alpha| = 1$ and $|\alpha| > 1$.

	$\lvert\alpha\rvert < 1$	$\lvert\alpha\rvert = 1$	$\lvert\alpha\rvert > 1$
Upper bound	2	2	$2\lvert\alpha\rvert^n$
Lower bound	$1 - \lvert\alpha\rvert$	n^{-k_α}	$\lvert\alpha\rvert^n - 1$

For an upper bound we have

$$\begin{aligned}\log(|A_n|) &= \sum_{\alpha\in\rho(f)} \log(|\alpha^n - 1|) \leq \sum_{\substack{\alpha\in\rho(f)\\|\alpha|\leq 1}} \log(2) + \sum_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} \log(2|\alpha|^n)\\ &= \sum_{\alpha\in\rho(f)} \log(2) + \sum_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} \log(|\alpha|^n) = n\log(\mathrm{M}(f)) + A.\end{aligned}$$

and for a lower bound we have

$$\begin{aligned}\log(|A_n|) &= \sum_{\alpha\in\rho(f)} \log(|\alpha^n - 1|)\\ &\geq \sum_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} \log(1-|\alpha|) + \sum_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} \log(n^{-k_\alpha}) + \sum_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} \log(|\alpha|^n - 1)\\ &\geq n\log(\mathrm{M}(f)) - A - B\log(n),\end{aligned}$$

for appropriately chosen constants A and B. Using these bounds we now find a lower bound for $\log(|a_n|)$. First we have

$$\sum_{d|n} \log(|a_d|) = \log(|A_n|) \quad \text{and therefore} \quad \log(|a_n|) = \sum_{d|n} \log(|A_d|)\,\mu(n/d).$$

This gives

$$\begin{aligned}\log(|a_n|) &= \sum_{d|n} \log(|A_d|)\mu(n/d) = \sum_{\substack{d|n\\\mu(n/d)=1}} \log(|A_d|) - \sum_{\substack{d|n\\\mu(n/d)=-1}} \log(|A_d|)\\ &\geq \sum_{\substack{d|n\\\mu(n/d)=1}} (d\log(\mathrm{M}(f)) - A - B\log(d)) - \sum_{\substack{d|n\\\mu(n/d)=-1}} (d\log(\mathrm{M}(f)) + A)\\ &= \log(\mathrm{M}(f)) \sum_{d|n} d\mu(n/d) - \sum_{d|n} A - \sum_{\substack{d|n\\\mu(n/d)=1}} B\log(d)\\ &\geq \varphi(n)\log(\mathrm{M}(f)) - \mathrm{d}(n)(A + B\log(n)).\end{aligned}$$

Finally, as $\varphi(n)$ grows faster than $n^{1-\varepsilon}$ for all $\varepsilon > 0$, and $\mathrm{d}(n)$ grows slower than n^{ε} for all $\varepsilon > 0$, the result follows. □

We now have a lower bound showing that $|a_n|$ grows exponentially. We now aim to find an upper bound on $|a_n|$ when a_n has no primitive prime divisors. We shall proceed by considering the entry of prime divisors p such that $f(x)$ has distinct roots in $\mathrm{GF}(p)$, i.e. primes p such that $p \nmid \Delta_f$ where Δ_f is the discriminant of $f(x)$.

In the following, we let $\delta = \deg(f)$ be the degree of $f(x)$ and Δ_f be the discriminant of $f(x)$. We aim to prove the following lemma.

Lemma 6.63. *If $p \nmid \Delta_f$, $p \mid a_n$ and $p \mid n$ then $p^{\delta+1} \nmid a_n$.*

In other words, if $p \nmid \Delta_f$ is a non-primitive prime divisor of a_n then p^δ is the largest power of p that can divide a_n, so if a_n contains no primitive prime divisors, and $(a_n, \Delta_f) = 1$, then $|a_n| \leq \mathrm{rad}(n)^\delta$. In order to prove this lemma, we shall begin by considering the case that $f(x)$ splits in $\mathrm{GF}(p)$. We will subsequently show that our method may be generalised to address the other cases in which $p \nmid \Delta_f$. First we quote Hensel's Lemma, which we shall use and subsequently generalise.

Lemma 6.64 (Hensel's Lemma)**.** *If α is a root of $f(x)$ in $\mathbb{Z}/p^k\mathbb{Z}$ then there is a unique root $\hat{\alpha} \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ of $f(x)$ such that $\hat{\alpha} \equiv \alpha \pmod{p^k}$.*

Proof. From the Taylor expansion of $f(x)$ in $\mathbb{Z}$ we have the equality

$$f(x+nh) = f(x) + nhf'(x) + (nh)^2 f''(x) + \dots.$$

If $n = p^k$ and we consider this expression modulo p^{k+1} we have the equality

$$f(x+p^k h) \equiv f(x) + p^k h f'(x) \pmod{p^{k+1}}.$$

Now suppose that α is a root of $f(x)$ modulo p^k. We therefore have $f(\alpha) = ap^k \pmod{p^{k+1}}$ for some a. As $p \nmid \Delta_f$, $f(x)$ does not have repeated roots modulo p, and so $f'(\alpha) \neq 0 \pmod{p}$. Hence, $f(\alpha + p^k h) \equiv 0 \pmod{p^{k+1}}$ if, and only if, h is the solution of $a = f'(\alpha)h \pmod{p}$. This shows that there is a unique root $\hat{\alpha}$ of $f(x)$ modulo p such that $\hat{\alpha} \equiv \alpha \pmod{p^k}$. □

If $\alpha \in \mathbb{Z}/p^k\mathbb{Z}$ is a root of $f(x)$ then we will call the root $\hat{\alpha} \in \mathbb{Z}/p^{k+1}\mathbb{Z}$ of $f(x)$ such that $\hat{\alpha} \equiv \alpha \pmod{p^k}$ the *lift* of α. Due to Hensel's Lemma we may identify a root α of $f(x)$ modulo p with all of its lifts. We now consider the sequence of lifts $\alpha_1, \alpha_2, \dots$ such that each α_i is a root of $f(x)$ in $\mathbb{Z}/p^i\mathbb{Z}$. Trivially, as $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$ we have that $\mathrm{ord}(\alpha_1) \mid p-1$. Letting $b = \mathrm{ord}(\alpha_1)$ we now give the following lemma.

Lemma 6.65. *There exists some number k such that*
$\mathrm{ord}(\alpha_1) = \mathrm{ord}(\alpha_2) = \dots = \mathrm{ord}(\alpha_k) = b$ *and* $\mathrm{ord}(\alpha_{k+i}) = p^i b$.

Proof. In the following we denote by $\delta, \delta', \dots$ arbitrary constants, and by $\varepsilon, \varepsilon', \dots$ arbitrary constants satisfying $\varepsilon \neq 0 \pmod{p}$. First, we show that if $\mathrm{ord}(\alpha_i) = b$ in

$\mathbb{Z}/p^i\mathbb{Z}$ then $\operatorname{ord}(\alpha_{i+1})$ is either b or pb in $\mathbb{Z}/p^{i+1}\mathbb{Z}$. We have

$$\alpha_{i+1}^{pb} \equiv ((\alpha_i + p^i\delta)^b)^p \equiv (\alpha_i^b + p^i\delta')^p \equiv (1 + p^i\delta'')^p \equiv 1 \pmod{p^{i+1}}.$$

Hence we see that $\operatorname{ord}(\alpha_{i+1}) \mid pb$, and as $\alpha_{i+1} \equiv \alpha_i \pmod{p^i}$ we know that $b \mid \operatorname{ord}(\alpha_{i+1})$, so $\operatorname{ord}(\alpha_{i+1})$ is either b or pb.

Now suppose that there is no k such that $\operatorname{ord}(\alpha_{k+1}) = pb$. If this is true, then for all i we have

$$A_b \equiv \prod_{\alpha\in\rho(f)} (\alpha^b - 1) \equiv (\alpha_i^b - 1) \prod_{\beta\in\rho(f)\setminus\{\alpha_i\}} (\beta^b - 1) \equiv 0 \pmod{p^i}.$$

As $A_b \in \mathbb{Z}$ we can only have $A_b \equiv 0 \pmod{p^i}$ for all i if $A_b = 0$. However, by assumption we know that no $\Phi_n(x) \mid f(x)$, so $f(x)$ has no root α satisfying $\alpha^n = 1$, hence we cannot have $A_n = 0$ for any n. Therefore, there exists some minimal k such that $\operatorname{ord}(\alpha_1) = \operatorname{ord}(\alpha_2) = \cdots = \operatorname{ord}(\alpha_k) = b$ and $\operatorname{ord}(\alpha_{k+1}) = pb$.

Now we show by induction that $\operatorname{ord}(\alpha_{k+i}) = p^i b$, with the base case of $i = 1$ as above. Given the hypothesis for $\operatorname{ord}(\alpha_{k+i})$ we have

$$\begin{aligned}\alpha_{k+i+1}^{p^i b} &\equiv ((\alpha_{k+1} + p^{k+1}\delta)^b)^{p^i} \equiv (\alpha_{k+1}^b + p^{k+1}\delta')^{p^i} \equiv ((1 + p^k\varepsilon) + p^{k+1}\delta')^{p^i} \\ &\equiv (1 + p^k\varepsilon')^{p^i} \equiv 1 + p^{k+i}\varepsilon' \neq 1 \pmod{p^{k+i+1}}.\end{aligned}$$

Hence $\operatorname{ord}(\alpha_{k+i+1}) \neq p^i b$, but as $\alpha_{k+i+1} \equiv \alpha_{k+i} \pmod{p^i}$ we have $p^i b \mid \operatorname{ord}(\alpha_{k+i+1})$. Now, considering $\alpha_{k+i+1}^{p^{i+1}b}$ we have

$$\begin{aligned}\alpha_{k+i+1}^{p^{i+1}b} &\equiv ((\alpha_k + p^k\delta)^b)^{p^{i+1}} \equiv (\alpha_k^b + p^k\delta')^{p^{i+1}} \equiv ((1 + p^k\delta'') + p^k\delta')^{p^{i+1}} \\ &\equiv (1 + p^k\delta''')^{p^{i+1}} \equiv 1 \pmod{p^{k+i+1}}.\end{aligned}$$

Hence $\operatorname{ord}(\alpha_{k+i+1}) \mid p^{i+1}b$. Finally, as $p^i b \mid \operatorname{ord}(\alpha_{k+i+1}) \mid p^{i+1}b$ and $\operatorname{ord}(\alpha_{k+i+1}) \neq p^i b$ we must have $\operatorname{ord}(\alpha_{k+i+1}) = p^{i+1}b$. □

For a given sequence of roots we shall refer to the number b as the *base order* and the number k as the *base order multiplicity*. For each root α of $f(x)$ we now introduce a pair of sequences related to A_n and a_n. For a root α of $f(x)$ with base order b and base order multiplicity k we define the sequences $\Lambda(\alpha)_n$ and $\lambda(\alpha)_n$ as follows

$$\Lambda(\alpha)_n = \begin{cases} 0, & \text{if } \alpha^n \not\equiv 1 \pmod{p}, \\ \text{i}, & \text{where } i \text{ is the as large as possible such that } \alpha^n \equiv 1 \pmod{i}, \end{cases}$$

and

$$\lambda(\alpha)_n = \begin{cases} k, & \text{if } n = b, \\ 1, & \text{if } n = p^i b \text{ for some } i \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

We now related the sequences $\Lambda(\alpha)_n$ and $\lambda(\alpha)_n$ by the following lemma.

Lemma 6.66. $\Lambda(\alpha)_n = \sum_{d|n} \lambda(\alpha)_d$.

Proof. We consider two cases. For $b \nmid n$ we have that $\Lambda(\alpha)_n = 0$, and for each $d \mid n$ we have $\lambda(\alpha)_d = 0$. Hence, in this case we have $\Lambda(\alpha)_n = \sum_{d|n} \lambda(\alpha)_d$.

For $b \mid n$, we have that n is of the form $p^i bm$ for some m with $p \nmid m$. In this case, $\operatorname{ord}(\alpha_{k+i}) = p^i b \mid n$, but $\operatorname{ord}(\alpha_{k+i+1}) = p^{i+1} b \nmid n$. Hence p^i is the highest power of p such that $\alpha^n \equiv 1 \pmod{p^{k+i}}$, and so $\Lambda(\alpha)_n = k + i$. Evaluating $\sum_{d|n} \lambda(\alpha)_d$ we have

$$\sum_{d|n} \lambda(\alpha)_d = \sum_{d|p^i b} \lambda(\alpha)_d = \lambda(\alpha)_b + \sum_{j=1}^{i} \lambda(\alpha)_{p^j b} = k + i.$$

Therefore, in all cases we have $\Lambda(\alpha)_n = \sum_{d|n} \lambda(\alpha)_d$. □

We now define sequences Λ_n and λ_n as follows.

$$\Lambda_n = \sum_{\alpha \in \rho(f)} \Lambda(\alpha)_n \quad \text{and} \quad \lambda_n = \sum_{\alpha \in \rho(f)} \lambda(\alpha)_n.$$

These sequences will be important to us due to the following relationships.

Lemma 6.67. *The highest power of p dividing A_n is Λ_n.*

Proof. For each root α of $f(x)$ we have that $\alpha^n - 1 \equiv p^i \varepsilon \pmod{p^j}$ where $i = \Lambda(\alpha)_n$, $\varepsilon \not\equiv 0 \pmod{p}$ and j is taken to be arbitrarily large. Letting $\alpha, \beta, \ldots, \omega$ be the roots of $f(x)$ we have

$$A_n \equiv (\alpha^n - 1)(\beta^n - 1) \ldots (\omega^n - 1) \equiv p^{\Lambda(\alpha)_n} \varepsilon_\alpha p^{\Lambda(\beta)_n} \varepsilon_\beta \ldots p^{\Lambda(\omega)_n} \varepsilon_\omega \equiv p^{\Lambda_n} \varepsilon \pmod{p^j},$$

where each $\varepsilon_\iota \not\equiv 0 \pmod{p}$ and $\varepsilon \not\equiv 0 \pmod{p}$, and j is arbitrarily large. □

Lemma 6.68. *The highest power of p dividing a_n is λ_n.*

Proof. The relations $A_n = \prod_{d|n} a_d$ and $\Lambda_n = \sum_{d|n} \lambda_d$ uniquely define the sequences

a_n and λ_n. The sequence μ_n of highest powers of p dividing a_n is uniquely defined and satisfies $\sum_{d|n} \mu_d = \Lambda_n$ due to the previous lemma, and hence $\lambda_n = \mu_n$. □

We are now in a position to give our first result regarding non-primitive prime divisors of a_n.

Lemma 6.69. *If p is not a primitive prime divisor of a_n, then the highest power of p that can divide a_n is $p^{\deg(f)}$.*

Proof. As p is a not a primitive prime divisor of a_n we have that $p \mid n$. The power of p dividing a_n is given by λ_n. We have

$$\lambda_n = \sum_{\alpha \in \rho(f)} \lambda(\alpha)_n \leq \deg(f).$$

This is due to the fact $\lambda(\alpha)_n \leq 1$ when $p \mid n$. □

This demonstrates our argument providing a bound on the powers of non-primitive prime divisors p of a_n. However, in order to prove our current version of this bound we have had to assume that $f(x)$ splits in $\mathbb{Z}/p\mathbb{Z}$. We will now show that this assumption can be reduced to the assumption $p \nmid \Delta_f$, the discriminant of $f(x)$. In order to do this, we will need to consider the roots of $f(x)$ in rings other than $\mathbb{Z}/p^i\mathbb{Z}$. We shall call the rings we introduce *Galois rings* as they are constructed in a manner analogous to the Galois fields and share similar properties.

Let $f(x), g(x) \in \mathbb{Z}[x]$ such that $f(x)$ and $g(x)$ are irreducible in $\mathbb{Z}/p\mathbb{Z}$, $\deg(g) = e$ and $\deg(f) \mid e$. We define the ring R_k by $R_k = (\mathbb{Z}/p^k\mathbb{Z})[x]/\langle g(x) \rangle$. We note that $R_1 \cong \mathrm{GF}(p^e)$, and so $f(x)$ splits in R_1. For elements $\alpha = a_1 + a_2 x + \cdots + a_e x^{e-1} \in R_k$ and $\beta = b_1 + b_2 x + \cdots + b_e x^{e-1} \in R_{k+j}$ we will use the notation $\beta \equiv \alpha \pmod{p^k}$ to mean $a_i \equiv b_i \pmod{p^k}$ for all $1 \leq i \leq e$. We first must generalise Hensel's Lemma to these rings. Let α be an arbitrary root of $f(x)$ in R_1.

Lemma 6.70. *There is a unique sequence of roots $\alpha_1 = \alpha, \alpha_2, \ldots$ in $R_1, R_2, \ldots$ such that each α_i is a root of $f(x)$ and $\alpha_{i+1} \equiv \alpha_i \pmod{p^i}$.*

Proof. Suppose that $\alpha_1, \ldots, \alpha_k$ are the first elements of such a sequence. Again, from the Taylor expansion of $f(x)$ we have

$$f(x + p^k h) = f(x) + p^k h f'(x) \quad \text{in } R_{k+1}.$$

As α_k is a root of f in R_k we have

$$f(\alpha_k + p^k h) = f(\alpha_k) + p^k h f'(\alpha_k) = p^k(\delta + h f'(\alpha_k)) \quad \text{in } R_{k+1}.$$

Considering the expression $\delta + hf'(\alpha_k)$ modulo p, i.e. in $R_1 \cong \mathrm{GF}(p^e)$, we have that $f'(\alpha_k) \not\equiv 0 \pmod{p}$, as $f(x)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$, so there is a unique solution to the equation $\delta + hf'(\alpha_k) \equiv 0 \pmod{p}$. Hence there is a unique root of $f(x)$ in R_{k+1}, α_{k+1}, such that $\alpha_{k+1} \equiv \alpha_k \pmod{p^k}$. □

We now give a technical result allowing us to define Galois rings. Let $h(x) \in \mathbb{Z}[x]$ be an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}$ such that $\deg(h) = \deg(f)$. Define S_k by $S_k = (\mathbb{Z}/p^k\mathbb{Z})[x]/\langle h(x)\rangle$.

Lemma 6.71. *For all $k \geq 1$, $R_k \cong S_k$.*

Proof. First, fix an arbitrary root α of $g(x)$ in R_1 and let $\alpha_1, \alpha_2, \ldots$ be its sequence of lifts. We may think of R_k as an algebraic extension of $\mathbb{Z}/p^k\mathbb{Z}$ by adjoining the element α_k, a root of $g(x)$. Basic Galois theory tells us that such an algebraic extension is unique up to isomorphism. Trivially, we have $R_1 \cong \mathrm{GF}(p^e) \cong S_1$. Hence, let β be the image of α in an isomorphism from R_1 to S_1. We have that β is a root of $g(x)$ in S_1, so from the previous lemma we may let $\beta_1, \beta_2, \ldots$ be the sequence of lifts of β in $S_1, S_2, \ldots$. Finally, as S_k contains a root β_k of $g(x)$ we may consider S_k as an algebraic extension of $\mathbb{Z}/p^k\mathbb{Z}$ by adjoining a root of $g(x)$, and therefore isomorphic to R_k. □

We are now able to define Galois rings. For $k, e \geq 1$ and a prime p let $g(x) \in \mathbb{Z}[x]$ be a polynomial such that $g(x)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}$ and $\deg(g) = e$. The Galois ring $\mathrm{GR}(p, k, e)$ is the quotient ring $(\mathbb{Z}/p^k\mathbb{Z})[x]/\langle g(x)\rangle$. We note from the previous lemma that this defines the Galois ring $\mathrm{GR}(p, k, e)$ uniquely to isomorphism, and is thus well defined. We shall call e the *extension degree* and k the *characteristic power* of $\mathrm{GR}(p, k, e)$. We note the special cases $\mathrm{GR}(p, 1, e) \cong \mathrm{GF}(p^e)$ and $\mathrm{GR}(p, k, 1) \cong \mathbb{Z}/p^k\mathbb{Z}$.

Our previous argument concerning the powers of non-primitive prime divisors dividing a_n relied upon roots of $f(x)$; their lifts from the ring $\mathbb{Z}/p^k\mathbb{Z}$ to $\mathbb{Z}/p^{k+1}\mathbb{Z}$ and relationships modulo powers of p. With our new notation, these lifts become lifts from $\mathrm{GR}(p, k, 1)$ to $\mathrm{GR}(p, k+1, 1)$. We can now recreate the previous argument but considering roots in the more general setting of $\mathrm{GR}(p, k, e)$ and their lifts to $\mathrm{GR}(p, k+1, e)$. This allows us to apply the same argument to any case in which $f(x)$ splits in some extension field $\mathrm{GF}(p^e)$ of $\mathbb{Z}/p\mathbb{Z}$, and where $f(x)$ has no repeated roots. As the argument is entirely argument, we omit repeating it in full here. We now

summarise our main result concerning which powers of non-primitive prime divisors may divide a_n.

Proposition 6.72. *If $p \nmid \Delta_f$ and $p \mid n$, then $p^{\deg(f)}$ is the largest power of p that can divide a_n.*

Proof. All that we need to show now is that the condition $p \nmid \Delta_f$ is sufficient for us to apply our argument. If this is the case, then $\Delta_f \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ and so $f(x)$ has no repeated roots in $\mathbb{Z}/p\mathbb{Z}$. Then we may consider an extension $\mathrm{GF}(p^e)$ of $\mathbb{Z}/p\mathbb{Z}$ where $f(x)$ splits. Now we may apply the previous argument in the rings $\mathrm{GR}(p, k, e)$. □

We now give an example to show that this proposition does not always hold when $p \mid \Delta_f$.

Lemma 6.73. *There exist polynomials $f(x) \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$ such that a_n has a non-primitive prime divisor p satisfying $p \mid n$ and $p^{\deg(f)+1} \mid a_n$.*

Proof. Taking $f(x) = x^2 - x + 10$ we have $\Delta_f = -39 = -1 \times 3 \times 13$, so $3 \mid \Delta_f$, and we have $a_6 = 81 = 3^4$. Hence in this case 3 is a non-primitive prime divisor of a_6 and a higher power than $3^{\deg(f)+1} = 3^3 \mid a_6$. □

We require a further proposition to allow us to create a bound on the size of a_n containing no primitive prime divisors. Unfortunately, the proof of the proposition we now give is non-constructive.

Proposition 6.74. *For each prime p such that $p \mid \Delta_f$ there exists some number k such that $p^k \nmid a_{p^r n}$ for all $r \geq 1$ and all n.*

Proof. This result was proved in a personal communication from Sawin to the author [47]. In the following we use the *p-adic valuation*, $\mathrm{v}_p(\alpha)$, which is an extension of the function on integers defined by $\mathrm{v}_p(n) = k$ if $p^k \mid\mid n$ which satisfies the following properties.

i) if α is an algebraic number then $\mathrm{v}_p(\alpha)$ is defined;

ii) for all α, β we have $\mathrm{v}_p(\alpha\beta) = \mathrm{v}_p(\alpha) + \mathrm{v}_p(\beta)$;

iii) for all α, β such that $\mathrm{v}_p(\alpha) \neq \mathrm{v}_p(\beta)$ we have $\mathrm{v}_p(\alpha + \beta) = \min(\mathrm{v}_p(\alpha), \mathrm{v}_p(\beta))$.

We now consider some $n = mp^r$ where $p \nmid m$. We define the polynomial $g(x) \in \mathbb{Z}[x]$ by

$$g(x) = \prod_{\xi_a \in \rho(\Phi_m)} f(\xi_a x).$$

The fact that $g(x) \in \mathbb{Z}[x]$ may be seen as each coefficient of $g(x)$ is a symmetric polynomial in the roots of $\Phi_m(x)$. We now have

$$a_n = \prod_{\xi_n \in \rho(\Phi_n)} f(\xi_n) = \prod_{\substack{\xi_a \in \rho(\Phi_m) \\ \xi_b \in \rho(\Phi_{p^r})}} f(\xi_a \xi_b) = \prod_{\xi_b \in \rho(\Phi_{p^r})} g(\xi_b).$$

Further, we may define some polynomial $h(x) \in \mathbb{Z}[x]$ such that $h(x-1) = g(x)$ so that we have

$$a_n = \prod_{\xi_b \in \rho(\Phi_{p^r})} g(\xi_b) = \prod_{\xi_b \in \rho(\Phi_{p^r})} h(\xi_b - 1).$$

Now define k to be the smallest number such that the coefficient of x^k in $h(x)$ is not divisible by p. Note that such a k is guaranteed to exist as $h(x)$ is monic.

Now, we consider the p-adic valuation of a_n, i.e. the highest power of p dividing a_n. We have

$$\mathrm{v}_p(a_n) = \mathrm{v}_p\left(\prod_{\xi_b \in \rho(\Phi_{p^r})} h(\xi_b - 1) \right) = \sum_{\xi_b \in \rho(\Phi_{p^r})} \mathrm{v}_p(h(\xi_b - 1))$$

We now consider each term $\mathrm{v}_p(h(\xi_b - 1))$. First, standard p-adic number theory gives us that $\mathrm{v}_p(\xi_b - 1) = 1/(p^r - p^{r-1}) = \varphi(p^r)^{-1}$. Let c_i denote the coefficient of x^i in $h(x)$. For $i < k$ we have $\mathrm{v}_p(c_i(\xi_b - 1)^i) = \mathrm{v}_p(c_i) + i\,\mathrm{v}_p(\xi_b - 1) > 1$, as we have $\mathrm{v}_p(c_i) \geq 1$ by assumption. For $i > k$ we have $\mathrm{v}_p(c_i(\xi_b - 1)^i) = \mathrm{v}_p(c_i) + i\,\mathrm{v}_p(\xi_b - 1) > k\,\varphi(p^r)^{-1}$, as $i > k$. Finally, we have $\mathrm{v}_p(c_k(\xi_b - 1)^k) = \mathrm{v}_p(c_k) + k\,\mathrm{v}_p(\xi_b - 1) = k\,\varphi(p^r)^{-1}$, as $\mathrm{v}_p(c_k) = 0$ by assumption. Now, as k is independent of r we may choose r large enough such that $k\,\varphi(p^r)^{-1} < 1$, which then gives us $\min_i(\mathrm{v}_p(c_i(\xi_b - 1)^i))$ is achieved uniquely for $i = k$, and hence $\mathrm{v}_p(h(\xi_b - 1)) = k\,\varphi(p^r)^{-1}$. Finally, we have

$$\mathrm{v}_p(a_n) = \sum_{\xi_b \in \rho(\Phi_{p^r})} \mathrm{v}_p(h(\xi_b - 1)) = \sum_{\xi_b \in \rho(\Phi_{p^r})} k\,\varphi(p^r)^{-1} = \varphi(p^r)(k\,\varphi(p^r)^{-1}) = k.$$

Altogether this shows for each prime p and number m such that $p \nmid m$, there is a computable k such that $p^k \mid\mid a_{mp^r}$ for sufficiently large r. We arrive at the final statement of this proposition by noting that for any prime p there are finitely many m such that $p \nmid m$ and $p \mid a_m$. □

We now may combine these two propositions to give a bound on a_n with no primitive prime divisors.

Proposition 6.75. *There exists some $k \in \mathbb{N}$ such that if a_n contains no primitive prime divisors then $|a_n| \leq \mathrm{rad}(n)^k$.*

Proof. With our assumptions on $f(x)$ we know that the discriminant Δ_f of $f(x)$ is non-zero, as $f(x)$ is irreducible in $\mathbb{Z}[x]$ and thus has no repeated roots. Therefore there are only finitely many primes p dividing Δ_f. For each prime p dividing Δ_f define k_p to be the smallest k derived from Proposition 6.74. Now, using Proposition 6.72 define k by $k = \max(\deg(f), \max_{p|\Delta_f}(k_p))$. □

We are now in a position to give our first result regarding roots of $f(x)$ of given multiplicative order.

Proposition 6.76. *For any monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ there are only finitely many m such that $f(x)$ has no roots of multiplicative order m in any finite field.*

Proof. From Proposition 6.62 we have that there exist constants C and N such that $|a_n| > e^{C\sqrt{n}}$ for all $n > N$, and from Proposition 6.75 we have that there exists some k such that any a_n with no primitive prime divisors satisfies $|a_n| \leq \mathrm{rad}(n)^k \leq n^k$. Hence, letting N' be the smallest N' such that $e^{C\sqrt{n}} > n^k$ for all $n > N'$, we have for all $n > \max(N, N')$ that $|a_n| > e^{C\sqrt{n}} > n^k$, and so a_n must have at least one primitive prime divisor. From Lemma 6.59 we have that a_n has a primitive prime divisor p if, and only if, $f(x)$ has a root of order n in a finite field of characteristic p. □

This allows us to give our first general result regarding (k, l, m)-regular maps with automorphism group a fractional linear group.

Proposition 6.77. *For each $k, l \in \mathbb{N}$ such that $k, l \geq 3$ and k, l is a hyperbolic pair, there are only finitely many m such that there are no (k, l, m)-regular maps with automorphism group a fractional linear group.*

Proof. We have that there is a (k, l, m)-regular map with automorphism group a fractional linear group if, and only if, $f_{k,l}(x)$ has a root of multiplicative order m in some finite field. By Lemma 6.58 we know that each $f_{k,l}(x)$ has at least one monic factor $g(x)$ such that $g(x)$ is irreducible, $g(x) \neq x$ and $g(x) \neq \Phi_n(x)$ for any n. Now we may apply Proposition 6.76 to $g(x)$ to deduce there are only finitely many m such that $g(x)$ has no roots of multiplicative order m in any finite field. Clearly as all roots of $g(x)$ are roots of $f_{k,l}(x)$ the result immediately follows. □

6.5 Constructive Cases

Following on from our previous section, we now aim to strengthen the bounds we used and make them constructive in order to explicitly calculate sets of orders for which a given polynomial $f(x)$ has no roots of that order. We begin by strengthening our lower bound. In order to do this, we require a theorem of Mignotte and Waldschmidt from [42]. First we shall require some definitions.

We shall define the *absolute logarithmic height* of an algebraic number α, denoted $\mathrm{h}(\alpha)$, where α has minimal polynomial

$$f(x) = c_0 x^d + c_1 x^{d-1} + \cdots + c_d = c_0 \prod_{\beta \in \rho(f)} (x - \beta),$$

by

$$\mathrm{h}(\alpha) = \frac{1}{d}\left(\log c_0 + \sum_{\alpha \in \rho(f)} \log \max(1, |\alpha|) \right).$$

Theorem 6.78 (Mignotte, Waldschmidt)**.** *If*

i) α_1, α_2 *are two non-zero algebraic numbers,*

ii) $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$*,*

iii) $\log \alpha_i$ *is any non-zero determination of the logarithm of* α_i *for* $i = 1, 2$*,*

iv) b_1 *and* b_2 *are positive rational integers such that* $b_1 \log \alpha_1 \neq b_2 \log \alpha_2$*,*

v) $B = \max(b_1, b_2)$*,*

vi) a_1, a_2 *and* f *are any real numbers satisfying*

  i) $a_i \geq 1$ *for* $i = 1, 2$*,*

  ii) $a_i \geq \mathrm{h}(\alpha_i) + \log 2$ *for* $i = 1, 2$*,*

  iii) $a_i = f|\log \alpha_i|/D$ *for* $i = 1, 2$*,*

  iv) $f \geq 2e$*.*

then

$$|b_1 \log \alpha_1 - b_2 \log \alpha_2| \geq e^{-270 D^4 a_1 a_2 (7.5 + \log B)^2}.$$

We first use this theorem to create a lemma more suited to our purposes. The following lemma is a common result given in relation to Baker's theorem. We quote it

here both for completeness and to show how we may explicitly calculate the constants involved. We reproduce the proof from [23].

Lemma 6.79. *If α is an algebraic number with absolute value 1 and minimal polynomial $f(x) \in \mathbb{Z}[x]$ then there is an explicitly computable constant A_α such that* $\log|\alpha^n - 1| \geq -A_\alpha(7.5 + \log n)^2 - \log 2$.

Proof. Choose a branch of the complex logarithm such that, for a complex number z, we have $\log z = \log|z| + i \arg z$ where $-\pi < \arg z \leq \pi$. This gives us the expansion $\log(z+1) = \sum_{k=1}^{\infty}(-1)^{k-1}z^k/k$ for $|z| < 1$. From this expansion one gets the inequality $|\log(z+1)| \leq 2|z|$ for $|z| \leq 1/2$. We now take $z = \alpha^n - 1$. If $|z| > 1/2$ then the statement is trivial, so we may assume $|z| \leq 1/2$. Hence we have

$$\log(z+1) = \log\alpha^n = n\log\alpha + 2k\pi i = n\log\alpha + k\log 1,$$

for some k, where we choose an determination of the logarithm in which $\log 1 = 2\pi i$. We may now apply Theorem 6.78 with

i) $\alpha_1 = \alpha$ and $\alpha_2 = 1$,

ii) $D = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f)$,

iii) $\log\alpha_1 = i\arg\alpha$ where $-\pi < \arg\alpha \leq \pi$ and $\log\alpha_2 = 2\pi i$,

iv) $b_1 = n$ and $b_2 = k$,

v) $B = \max(b_1, b_2) = n$ (as we may choose the determination of $\log\alpha^n = \log|\alpha^n| + i\arg|\alpha^n|$ where $-\pi < \arg|\alpha^n| \leq \pi$),

vi) a_1, a_2 and f are real numbers as described in Theorem 6.78.

Applying Theorem 6.78 we now get

$$|\log(z+1)| = |n\log\alpha + k\log 1| \geq \exp(-270D^4a_1a_2(7.5 + \log n)^2).$$

As $|z| \leq 1/2$, we have $|\log(z+1)| \leq 2|z| = 2|\alpha^n - 1|$. Therefore we have

$$2|\alpha^n - 1| \geq e^{-270D^4a_1a_2(7.5+\log n)^2},$$

and so

$$\log|\alpha^n - 1| \geq -270D^4a_1a_2(7.5 + \log n)^2 - \log 2.$$

Taking $A_\alpha = 270D^4a_1a_2$ gives the result. □

We now use this to create a bound on terms $\Phi_n(\alpha)$ where α is an algebraic number with $|\alpha| = 1$.

Lemma 6.80. *If α is the root of an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(x) \neq x$ and $f(x) \neq \Phi_n(x)$ for any n, and $|\alpha| = 1$, then $|\Phi_n(\alpha)| \geq \exp(-\operatorname{d}(n)(A_\alpha(7.5 + \log n)^2 + \log 2))$ for some explicitly computable constant A_α depending only on α.*

Proof. From the relation $|\alpha^n - 1| = \prod_{d|n} |\Phi_d(\alpha)|$ we have $|\Phi_n(\alpha)| = \prod_{d|n} |\alpha^d - 1|\,\mu(n/d)$. Hence we have $\log|\Phi_n(\alpha)| = \sum_{d|n} \log|\alpha^d - 1|\,\mu(n/d)$. As $\log|\alpha^k - 1| \leq \log 2$ for all k, and

$$\log|\alpha^k - 1| \geq -A_\alpha(7.5 + \log k)^2 - \log 2 \geq -A_\alpha(7.5 + \log n)^2 - \log 2$$

for all k, we have

$$\begin{aligned}
\log|\alpha^n - 1| = \sum_{d|n} |\alpha^d - 1|\,\mu(n/d) &= \sum_{\substack{d|n \\ \mu(n/d)=1}} |\alpha^d - 1| - \sum_{\substack{d|n \\ \mu(n/d)=-1}} |\alpha^d - 1| \\
&\geq \sum_{\substack{d|n \\ \mu(n/d)=1}} (-A_\alpha(7.5 + \log n)^2 - \log 2) - \sum_{\substack{d|n \\ \mu(n/d)=-1}} \log 2 \\
&= \sum_{\substack{d|n \\ \mu(n/d)=1}} -A_\alpha(7.5 + \log n)^2 - \sum_{d|n} \log 2 \\
&\geq -\operatorname{d}(n)(A_\alpha(7.5 + \log n)^2 + \log 2).
\end{aligned}$$

The result follows immediately. □

This addresses the most difficult case of finding a lower bound for terms of the form $\Phi_n(\alpha)$ when $|\alpha| = 1$. These terms are intuitively difficult to create a lower bound for as α is a point on the unit circle, and as it is not a root of unity its powers will get arbitrarily close to roots of unity infinitely often. We now need to create lower bounds for terms of the form $\Phi_n(\alpha)$ when $|\alpha| > 1$ and $|\alpha| < 1$, both of which are considerably simpler. We begin with a lower bound for $\Phi_n(\alpha)$ when $|\alpha| < 1$.

Lemma 6.81. *For all $|z| < 1$ we have $|1/(1 - z)| \geq 1 - |z|$.*

Proof. $1/(1 - z) \geq 1/(1 + |z|) = (1 - |z|)/(1 - |z|^2) \geq 1 - |z|$. □

Lemma 6.82. *For all $z \in \mathbb{C}$ such that $|z| < 1$, we have $|\Phi_n(z)| \geq \exp(-(1 - |z|)^{-3/2})$.*

Proof. First, we have the identity

$$\Phi_n(z) = \prod_{d|n} (z^d - 1)^{\mu(n/d)}.$$

Noting Lemma 6.81 and the fact $|1 - z| \geq 1 - |z|$, we have

$$|\Phi_n(z)| = \prod_{d|n} |z^d - 1| = \prod_{d|n} |1 - z^d| \geq \prod_{d|n} (1 - |z|^d) \geq \prod_{n=1}^{\infty} (1 - |z|^n).$$

We now note the inequality

$$\log(1 - x) \geq \frac{-x}{\sqrt{1 - x}}$$

for all $0 \leq x < 1$. Letting $\alpha = |z|$, we have

$$\log\left(\prod_{n=1}^{\infty} (1 - \alpha^n)\right) = \sum_{n=1}^{\infty} \log(1 - \alpha^n) \geq -\sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{1 - \alpha^n}}.$$

From $0 \leq \alpha < 1$ we have $\sqrt{1 - \alpha^n} \geq \sqrt{1 - \alpha}$, $1/\sqrt{1 - \alpha^n} \leq 1/\sqrt{1 - \alpha}$ and therefore $-1/\sqrt{1 - \alpha^n} \geq -1/\sqrt{1 - \alpha}$, so we have

$$-\sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{1 - \alpha^n}} \geq -\sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{1 - \alpha}} \geq -\frac{1}{\sqrt{1 - \alpha}} \sum_{n=1}^{\infty} \alpha^n = -(1 - \alpha)^{-3/2}.$$

Altogether this gives

$$\log|\Phi_n(z)| \geq -(1 - |z|)^{-3/2} \quad \Leftrightarrow \quad |\Phi_n(z)| \geq \exp(-(1 - |z|)^{-3/2}). \qquad \square$$

We are now in a position to give our lower bound on the terms a_n. We will begin with the case where $f(x)$ has no roots α such that $|\alpha| = 1$.

Proposition 6.83. *If $f(x) \in \mathbb{Z}[x]$ satisfies $x \nmid f(x)$ and $\Phi_n(x) \nmid f(x)$ for any n, and $f(x)$ has no roots α such that $|\alpha| = 1$, then there is a computable constant C such that $|a_n| \geq C\,\mathrm{M}(f)^{\varphi(n)}$ where $\mathrm{M}(f)$ is the Mahler measure of $f(x)$.*

Proof. We have

$$a_n = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha) = \prod_{\substack{\alpha \in \rho(f) \\ |\alpha| > 1}} \alpha^{\varphi(n)} \Phi_n(\alpha^{-1}) \prod_{\substack{\alpha \in \rho(f) \\ |\alpha| < 1}} \Phi_n(\alpha).$$

From Lemma 6.82 we may take

$$C = \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} e^{-(1-|\alpha^{-1}|)^{-3/2}} \prod_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} e^{-(1-|\alpha|)^{-3/2}},$$

and we have

$$\begin{aligned}|a_n| &= \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} |\alpha^{\varphi(n)}\Phi_n(\alpha^{-1})| \prod_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} |\Phi_n(\alpha)| \\ &= \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} |\alpha^{\varphi(n)}| \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} |\Phi_n(\alpha^{-1})| \prod_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} |\Phi_n(\alpha)| \\ &\geq C \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} |\alpha^{\varphi(n)}| = C\,\mathrm{M}(f)^{\varphi(n)}.\end{aligned}$$

□

We now give our lower bound for $|a_n|$ in the more complex case in which there exist roots α of $f(x)$ such that $|\alpha| = 1$.

Lemma 6.84. *If $f(x) \in \mathbb{Z}[x]$ satisfies $x \nmid f(x)$ and $\Phi_n(x) \nmid f(x)$ for any n then there are computable constants A, B and C such that*

$$|a_n| \geq C\,\mathrm{M}(f)^{\varphi(n)} e^{-\mathrm{d}(n)(A(7.5+\log n)^2+B\log 2)}.$$

Proof. As before, from Lemma 6.82 we have

$$\begin{aligned}|a_n| &= \prod_{\alpha\in\rho(f)} |\Phi_n(\alpha)| = \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} |\Phi_n(\alpha)| \prod_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} |\Phi_n(\alpha)| \prod_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} |\Phi_n(\alpha)| \\ &= \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} (|\alpha|^{\varphi(n)}|\Phi_n(\alpha^{-1})|) \prod_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} |\Phi_n(\alpha)| \prod_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} |\Phi_n(\alpha)| \\ &\geq C\,\mathrm{M}(f)^{\varphi(n)} \prod_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} |\Phi_n(\alpha)|,\end{aligned}$$

where C is given by

$$C = \prod_{\substack{\alpha\in\rho(f)\\|\alpha|>1}} e^{-(1-|\alpha^{-1}|)^{-3/2}} \prod_{\substack{\alpha\in\rho(f)\\|\alpha|<1}} e^{-(1-|\alpha|)^{-3/2}}.$$

We now use Lemma 6.80 to bound the terms of the form $|\Phi_n(\alpha)|$. From this lemma,

for each α there exists some A_α depending only on α such that

$$|\Phi_n(\alpha)| \geq e^{-\mathrm{d}(n)(A_\alpha(7.5+\log n)^2+\log 2)}.$$

Hence we have

$$\begin{aligned}|a_n| &\geq C\,\mathrm{M}(f)^{\varphi(n)} \prod_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} |\Phi_n(\alpha)| \\ &\geq C\,\mathrm{M}(f)^{\varphi(n)} \prod_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} e^{-\mathrm{d}(n)(A_\alpha(7.5+\log n)^2+\log 2)} \\ &\geq C\,\mathrm{M}(f)^{\varphi(n)} e^{-\mathrm{d}(n)(A(7.5+\log n)^2+B\log 2)},\end{aligned}$$

where

$$A = \sum_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} A_\alpha \quad \text{and} \quad B = \sum_{\substack{\alpha\in\rho(f)\\|\alpha|=1}} 1. \qquad \square$$

In order to use these bounds we are going to need easily usable bounds on the totient function $\varphi(n)$ and the divisors function $\mathrm{d}(n)$. Standard number theory tells us that $\varphi(n) \sim n^{1-\varepsilon}$ for all $\varepsilon > 0$ and $\mathrm{d}(n) \sim n^\varepsilon$ for all $\varepsilon > 0$. Hence, we shall give arguments which allow us to calculate, for arbitrary $\varepsilon > 0$, explicit constants T_ε and D_ε such that $\varphi(n) \geq T_\varepsilon n^{1-\varepsilon}$ and $\mathrm{d}(n) \leq D_\varepsilon n^\varepsilon$.

Lemma 6.85. *For each $\varepsilon > 0$ there is a computable constant T_ε such that $\varphi(n) \geq T_\varepsilon n^{1-\varepsilon}$.*

Proof. For each prime p we aim to find a constant β_p such that $\varphi(p^k) \geq \beta_p (p^k)^{1-\varepsilon}$. Let α be the smallest number such that for all $x \geq \alpha$ we have $x \geq x^{1-\varepsilon} + 1$, which we know to exist as $1 - \varepsilon < 1$.

For $p > \alpha$ we have

$$\varphi(p^k) = p^{k-1}(p-1) \geq p^{k-1}p^{1-\varepsilon} = p^{k-\varepsilon} \geq (p^k)^{1-\varepsilon}.$$

Hence taking $\beta_p = 1$ we have $\varphi(p^k) \geq \beta_p (p^k)^{1-\varepsilon}$.

For $p \leq \alpha$ let K_p be the smallest number such that $p^k(1-1/p) \geq (p^k)^{1-\varepsilon}$ for all $k \geq K_p$. Now take

$$\beta_p = \min_{1\leq i\leq K_p} \left\{ \frac{p^k(1-1/p)}{(p^k)^{1-\varepsilon}} \right\}.$$

This gives us

$$\varphi(p^k) = p^k(1-1/p) = \frac{p^k(1-1/p)}{(p^k)^{1-\varepsilon}}(p^k)^{1-\varepsilon} \geq \beta_p(p^k)^{1-\varepsilon}.$$

We may now take $T_\varepsilon = \prod \beta_p$ where the product is taken over all primes p. As there are only finitely many primes p such that $p \leq \alpha$, and for $0 < p \leq \alpha$ we have $0 < \beta_p < 1$ this product is well defined. Hence, for $n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ we have

$$\begin{aligned} T_\varepsilon n^{1-\varepsilon} &\leq \beta_{p_1}(p_1^{a_1})^{1-\varepsilon}\beta_{p_2}(p_2^{a_2})^{1-\varepsilon}\dots\beta_{p_k}(p_k^{a_k})^{1-\varepsilon} \\ &\leq p_1^{a_1}(1-1/p_1)p_2^{a_2}(1-1/p_2)\dots p_k^{a_k}(1-1/p_k) = \varphi(n). \end{aligned}$$

The result follows from the fact we may easily compute α and then use this to compute T_ε. □

Lemma 6.86. *For each $\varepsilon > 0$ there is a computable constant D_ε such that $\mathrm{d}(n) \leq D_\varepsilon n^\varepsilon$.*

Proof. As before, we first prove for each prime p and $\varepsilon > 0$ there exists a computable constant β_p such that $\mathrm{d}(p^k) \leq \beta_p(p^k)^\varepsilon$.

First, letting $\alpha = 2^{1/\varepsilon}$, if $p \geq \alpha$ then we have $\mathrm{d}(p^k) = k+1$ and $(p^k)^\varepsilon \geq 2^k \geq k+1$. Therefore for all $p \geq \alpha$ we may take $\beta_p = 1$ and we have $\mathrm{d}(p^k) \leq \beta_p(p^k)^\varepsilon$.

For $p < \alpha$, we now define K_p to be the smallest integer such that $(p^\varepsilon)^k \geq k+1$ for all $k \geq K_p$ which we know to exist as $p^\varepsilon > 1$. Now we take

$$\beta_p = \max_{1 \leq i \leq K_p} \left\{ \frac{i+1}{(p^\varepsilon)^i} \right\}.$$

Hence we have

$$\beta_p(p^k)^\varepsilon = \beta_p(p^\varepsilon)^k \geq \left(\frac{k+1}{(p^\varepsilon)^k}\right)(p^\varepsilon)^k = k+1.$$

We now may take $D_\varepsilon = \prod \beta_p$ where the product is taken over all primes p. As there are only finitely many primes p such that $p < \alpha$, and for all $p < \alpha$ we have that $1 < \beta_p < \infty$, the product D_ε is well defined. Hence, for $n = p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ we have

$$\begin{aligned} D_\varepsilon n^\varepsilon &\geq \beta_{p_1}(p_1^{a_1})^\varepsilon\beta_{p_2}(p_2^{a_2})^\varepsilon\dots\beta_{p_k}(p_k^{a_k})^\varepsilon \\ &\geq (a_1+1)(a_2+1)\dots(a_k+1) = \mathrm{d}(n). \end{aligned}$$

The result follows as we may easily compute α and then use this to compute D_ε. □

We now have all the material required to create our first explicit lower bounds on the terms $|a_n|$, so we now work to make our upper bound on terms $|a_n|$ with no primitive prime divisors explicit. To do this, for a polynomial $f(x) \in \mathbb{Z}[x]$ we consider each prime $p \mid \Delta_f$ and determine an upper bound on which powers of p may divide terms $|a_n|$. We first require a definition. For a monic polynomial $f(x) \in \mathbb{Z}[x]$ given by $f(x) = x^n - a_n x^{n-1} - \cdots - a_1$ we define the *companion matrix* $C \in \mathbb{M}^n$ of $f(x)$ to be the matrix

$$C = \begin{pmatrix} 0 & 0 & 0 & \dots & a_1 \\ 1 & 0 & 0 & \dots & a_2 \\ 0 & 1 & 0 & \dots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}.$$

Lemma 6.87. *If C is the companion matrix of an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$, then for any polynomial $g(x) \in \mathbb{Z}[x]$ we have* $\operatorname{Det}(g(C)) = \prod_{\alpha \in \rho(f)} g(\alpha)$.

Proof. The companion matrix of $f(x)$ is similar to the diagonal matrix D given by

$$D = \begin{pmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_n \end{pmatrix},$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the roots of $f(x)$. Hence there exists some matrix Q such that $C = Q^{-1}DQ$. Noting that
$C^n = (Q^{-1}DQ)^n = Q^{-1}DQQ^{-1}DQ \dots Q^{-1}DQ = Q^{-1}D^nQ$, we have

$$\begin{aligned} \operatorname{Det}(g(C)) &= \operatorname{Det}(g(Q^{-1}DQ)) = \operatorname{Det}(Q^{-1}g(D)Q) = \operatorname{Det}(Q^{-1})\operatorname{Det}(g(D))\operatorname{Det}(Q) \\ &= \operatorname{Det}\left(\begin{pmatrix} g(\alpha_1) & 0 & 0 & \dots & 0 \\ 0 & g(\alpha_2) & 0 & \dots & 0 \\ 0 & 0 & g(\alpha_3) & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & g(\alpha_n) \end{pmatrix}\right) = \prod_{\alpha \in \rho(f)} g(\alpha), \end{aligned}$$

as $\operatorname{Det}(Q^{-1})\operatorname{Det}(Q) = 1$. □

Letting $A_n = \prod_{\alpha \in \rho(f)} (\alpha^n - 1)$ and $a_n = \prod_{\alpha \in \rho(f)} \Phi_n(\alpha)$ as before this gives the following important corollary.

Corollary 6.88. *If $f(x) \in \mathbb{Z}[x]$ is an irreducible monic polynomial and C is the companion matrix of $f(x)$ then $A_n = \mathrm{Det}(C^n - I)$ and $a_n = \mathrm{Det}(\Phi_n(C))$.*

Proof. Immediate. □

In light of this lemma we now give a method to, for a given prime p, calculate a bound on powers of p dividing terms of the form a_n. In the following we make the further assumption that we are considering an irreducible, monic polynomial $f(x) \in \mathbb{Z}[x]$ in which the discriminant Δ_f and the constant coefficient of $f(x)$ are coprime.

Lemma 6.89. *If $p \mid\mid n$ and $p \mid a_n$, then for each k there exists a computable number r such that $a_{p^i n} \not\equiv 0 \pmod{p^k}$ for any i if, and only if, $a_{p^i n} \not\equiv 0 \pmod{p^k}$ for all $0 \leq i \leq r$.*

Proof. As $p \mid\mid n$, from the identity of cyclotomic polynomials $\Phi_{p^r n}(x) = \Phi_n(x^{p^r})$ and the fact $a_m = \mathrm{Det}(\Phi_m(C))$ we have $a_{p^r n} = \mathrm{Det}(\Phi_n(C^{p^r}))$. By assumption, p is not a divisor of the constant coefficient of $f(x)$, which is given by $\mathrm{Det}(C)$, so C is not a zero divisor in any matrix ring over $\mathbb{Z}/p^k\mathbb{Z}$, and has multiplicative order bp^c for some b with $p \nmid b$. Therefore for $i \equiv j \pmod{p^c b}$ we have $C^i \equiv C^j \pmod{p^k}$. Hence, let k be a high enough power of p such that $p^k \nmid a_{np^r}$ for any r, which we know to exist by Lemma 6.74, and let bp^c be the multiplicative order of C in over $\mathbb{Z}/p^k\mathbb{Z}$. By the Chinese Remainder Theorem the sequence $p^r \pmod{bp^c}$ is determined uniquely by the sequences $p^r \pmod{b}$ and $p^r \pmod{p^c}$. For $r \geq c$, the sequence $p^r \equiv 0 \pmod{p^c}$, and the sequence $p^r \pmod{b}$ repeats with period the order of $p \pmod{b}$. Letting m be the order of $p \pmod{b}$, we see that for $r \geq c$, if $0 \leq r' < m$ and $r \equiv c + r' \pmod{m}$, then $a_{p^r n} \equiv p^{c+r'} n \pmod{p^k}$. Therefore, if $a_{p^r n} \not\equiv 0 \pmod{p^k}$ for all $r \leq m + c$, then $a_{p^r n} \not\equiv 0 \pmod{p^k}$ for all r. □

Due to the technical nature of the lemma, we provide an example to clarify the idea.

Example 6.90. For $f(x) = x^2 - x - 1$, if $p \mid n$ then $a_n \not\equiv 0 \pmod{p^3}$.

Proof. In this case we have $\Delta_f = 5$, so for all primes $p \neq 5$ we may apply Proposition 6.72. For the other case, we first have that $5 \mid a_n$ where $5 \nmid n$ if, and only if, there is a root of $f(x)$ of order n in $\mathbb{Z}/5\mathbb{Z}$. In $\mathbb{Z}/5\mathbb{Z}$ we have $f(x) = (x-3)^2$, so the only a_n such that $5 \mid a_n$ and $5 \nmid n$ is $n = 4$. We follow the previous lemma, taking $n = 4$ and $p = 5$. The companion matrix C of $f(x)$ is given by

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

We have that C has multiplicative order $500 = 2^2 \times 5^3$ modulo 5^3. Hence the sequence $5^r \pmod{4 \times 5^3}$ can be found by considering the sequences $5^r \pmod 4$ and $5^r \pmod{5^3}$. Clearly $5^r \equiv 1^r \equiv 1 \pmod 4$ and $5^r \equiv 0 \pmod{5^3}$ for $r \geq 3$. Hence, for all $r \geq 3$ we have

$$\begin{aligned} a_{20\times 5^r} &\equiv \mathrm{Det}(\Phi_{20\times 5^r}(C)) \equiv \mathrm{Det}(\Phi_{20}(C^{5^r})) \\ &\equiv \mathrm{Det}(\Phi_{20}(C^{5^3})) \equiv a_{20\times 5^3} \equiv a_{2500} \pmod{5^3} \end{aligned}$$

Hence we calculate $a_{20\times 5^t} \pmod{5^3}$ for $0 \leq r \leq 3$. We have

$$a_{20} \equiv 25, \quad a_{20\times 5} \equiv 25, \quad a_{20\times 5^2} \equiv 25, \quad \text{and} \quad a_{20\times 5^3} \equiv 25 \pmod{5^3}.$$

The result follows immediately. □

We will now give apply these lemmas to an example polynomial $f_{k,l}(x)$ and determine an explicit bound beyond which roots of all multiplicative orders exist to $f_{k,l}(x)$ in some finite field. First we require a bound on $|a_n|$ when a_n has no primitive prime divisors.

Lemma 6.91. *For $f_{3,7}(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1$, if a_n has no primitive prime divisors then $|a_n| \leq n^6$.*

Proof. First we calculate the discriminant Δ_f of $f(x)$ as $\Delta_f = 31,213 = 7^4 \times 13$. Hence for all primes $p \notin \{7, 13\}$ we may apply Proposition 6.72 to show that if $p \mid n$ then $p^7 \nmid a_n$.

We now consider the case $p = 7$. In this case, we have $f(x) = (x^2 + 3x + 1)^3$ in $(\mathbb{Z}/7\mathbb{Z})[x]$, so has only two distinct roots. The roots of $f(x)$ are both multiplicative order 8, so we have that if $7 \mid a_n$ then $n = 8 \times 7^i$ for some $i \geq 0$. Letting C be the companion matrix of $f(x)$ in GF(7) we have

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 6 \\ 1 & 0 & 0 & 0 & 0 & 5 \\ 0 & 1 & 0 & 0 & 0 & 5 \\ 0 & 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 0 & 1 & 5 \end{pmatrix}.$$

One can easily verify that the multiplicative order of C is 56. Hence, letting $m = \mathrm{ord}(C)$ in $\mathbb{Z}/7^7\mathbb{Z}$ we know that $56 \mid 7$ so one can easily verify $m = 7^6 \times 56$. We now use the relation $\Phi_{7^r\times 56}(x) = \Phi_{56}(x^{7^r})$ for all r to calculate each $a_{7^r\times 56}$. We

consider the values of $C^{7^r} \pmod{7^7}$, as C is order $7^7 \times 8$ we consider the values of $7^r \pmod{7^7 \times 8}$. For $r \geq 7$ we have $7^r \equiv 0 \pmod{7^7}$ and $7^r \equiv 1 \pmod 8$ if r is even and $7^r \equiv 7 \pmod 8$ if r is odd. Therefore for any $r > 8$ there exists some $0 \leq r' \leq 8$ such that $C^{7^r} \equiv C^{7^{r'}} \pmod{7^7}$. Therefore we calculate $a_{7^r \times 56} \equiv \mathrm{Det}(\Phi_{56}(C^{7^r})) \pmod{7^7}$ for $0 \leq r \leq 8$. We have $a_{7^r \times 56} \equiv \Phi_{56}(C^{7^r}) \equiv 7^6 \pmod{7^7}$ for all $0 \leq r \leq 8$, and therefore for all r. Hence if $7 \mid n$ then we have $7^7 \nmid a_n$.

We now consider the case $p = 13$. In this case, we have $f(x) = (x+12)^2(x+2)(x+7)(x^2+8x+1)$, from which we calculate the possible multiplicative orders of roots of $f(x)$ are 1, 12 and 14. Hence if $13 \mid a_n$ we must have $n = 13^r k$ for some $k \in \{1, 12, 14\}$ and $r \geq 0$. One can verify that the companion matrix C of $f(x)$ in $\mathbb{Z}/13\mathbb{Z}$ has multiplicative order $1092 = 84 \times 13$. Letting m be the multiplicative order of C over $\mathbb{Z}/13^3\mathbb{Z}$ we therefore easily see that $1092 \mid m$ so can easily verify that $m = 13^2 \times 1092$. We now consider the values of C^{13^r} in $\mathbb{Z}/13^3\mathbb{Z}$ for different powers of r. As C is order $13^3 \times 84$, we therefore consider the values of 13^r modulo $13^3 \times 84$. We have $13^r \equiv 0 \pmod{13^3}$ for all $r \geq 3$ and $13^r \equiv 1 \pmod{84}$ if r is even and $13^r \equiv 13 \pmod{84}$ if r is odd. Hence, for all $r > 4$ there exists some $0 \leq r' \leq 4$ such that $C^{13^r} \equiv C^{13^{r'}} \pmod{13^3}$. We now calculate $a_{13^r \times 13k}$ for $k \in \{1, 12, 14\}$ and $r \geq 0$. We have

$$\begin{aligned}
a_{13} \equiv a_{13^2} \equiv a_{13^3} \equiv a_{13^4} \equiv a_{13^5} \equiv 13^2 \pmod{13^3},\\
a_{156} \equiv a_{13\times 156} \equiv a_{13^2\times 156} \equiv a_{13^3\times 156} \equiv a_{13^4\times 182} \equiv 13^2 \pmod{13^3},\\
a_{182} \equiv a_{13\times 182} \equiv a_{13^2\times 182} \equiv a_{13^3\times 182} \equiv a_{13^4\times 182} \equiv 13^2 \pmod{13^3}.
\end{aligned}$$

Finally, any other $a_{13^r \times 13k}$ for $k \in \{1, 12, 14\}$ and $r \geq 0$ is equal to one of these, and therefore if $13 \mid n$ then $13^3 \nmid a_n$ and $13^7 \nmid a_n$.

Altogether we have for all primes that if $p \mid n$ then $p^7 \nmid a_n$. Hence, if a_n only has non-primitive prime divisors, we must have $|a_n| \leq \mathrm{rad}(n)^6 \leq n^6$, establishing our upper bound on a_n with no non-primitive prime divisors. □

We now compute explicit constants to give us a constructive lower bound on $|a_n|$.

Lemma 6.92. *We have*

$$\begin{aligned}
|a_n| &\geq C\,\mathrm{M}(f)^{\varphi(n)} e^{-\mathrm{d}(n)(A(7.5+\log n)^2 + B\log 2)}\\
&\geq C\,\mathrm{M}(f)^{\sqrt{n/2}} e^{-4n^{1/3}(a(7.5+\log n)^2 + B\log 2)},
\end{aligned}$$

where $A = 10,867,224.615\ldots$, $B = 4$, $C = 0.000259611\ldots$ *and* $\mathrm{M}(f) = 1.6355\ldots$.

Proof. We use Lemma 6.84. This immediately allows us to calculate B, C and $\mathrm{M}(f)$. To calculate A we use Lemma 6.79. The bounds for the totient function and the divisors function used are $\varphi(n) \geq \sqrt{n/2}$ and $\mathrm{d}(n) \leq 4n^{1/3}$, which may both be derived from the methods of Lemma 6.85 and Lemma 6.86. □

We are now in a position to give our first explicit existence result on roots of $f_{3,7}(x)$.

Proposition 6.93. *The polynomial $f_{3,7}(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1$ has at least one root of order m in some finite field for all $m \geq 10^{76}$.*

Proof. By combining Lemma 6.91 and Lemma 6.92 we can show that $|a_n| > n^6$ for all $n \geq 10^{76}$ and thus all $n \geq 10^{76}$ must have at least one primitive prime factor. □

We now aim to create a new, better bound which will allow us to show that all a_n for n in an interval up to 10^{76} have at least one primitive prime divisor. To do this, we shall use a method relying on using continued fraction expansions. The method we used can be found in [42]. We first require the following standard theorem of continued fractions, a proof of which may be found in [21].

Theorem 6.94. *If $[a_0; a_1, a_2, \dots]$ is a continued fraction expansion of α, and p_n/q_n are its convergents, then*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(a+2)q^2}$$

for all $q \leq q_n$ where $a = \max_{1 \leq i \leq n+1} a_i$.

We shall use this bound to create a lower bound on terms of the form $\Phi_n(\alpha)$ when $|\alpha| = 1$. First we give a bound on expressions of the form $|\alpha^n - 1|$.

Lemma 6.95. *Letting $\alpha = e^{i2\pi\beta}$ where $[a_0; a_1, a_2, \dots]$ is a continued fraction expansion of β with convergents p_n/q_n, for all $k \leq q_n$ we have $|\alpha^k - 1| \geq 2\pi/(a+2)k$ where $a = \max_{1 \leq i \leq n} a_i$.*

Proof. For any complex number z such that $|z| = 1$ we have $|\arg z| \geq |z - 1|$, where $-\pi < \arg z \leq \pi$, as $\arg z$ measures the distance along the unit circle from 1 to z and $|z - 1|$ measures the straight line distance from 1 to z. We have

$$\arg \alpha^n = \min_{m \in \mathbb{Z}}(n \arg \alpha - 2\pi m) = \min_{m \in \mathbb{Z}}(n2\pi\beta - 2\pi m).$$

Hence we have

$$|\alpha^n - 1| \geq |\arg \alpha^n| = \min_{m \in \mathbb{Z}}(n2\pi\beta - 2\pi m) = 2\pi n \min_{m \in \mathbb{Z}}\left(\beta - \frac{m}{n}\right) \geq \frac{2\pi n}{(a+2)n^2},$$

where finally we use Theorem 6.94 to bound the expression $\min_{m\in\mathbb{Z}}(\beta - m/n)$. □

We now may improve our bound on $|a_n|$ as follows.

Lemma 6.96. *There exist explicitly computable constants C, $\mathrm{M}(f)$ and a_α for each $\alpha \in \rho(f)$ with $|\alpha| = 1$ such that*

$$|a_n| \geq C\,\mathrm{M}(f)^{\varphi(n)} \left\{ \prod_{\substack{\alpha\in\rho(f)\\ |\alpha|=1}} \left(\frac{2\pi}{(a_\alpha+2)n}\right)^{\mathrm{d}(n)} \right\}$$
$$\geq C\,\mathrm{M}(f)^{(1/5)n^{49/50}} \left\{ \prod_{\substack{\alpha\in\rho(f)\\ |\alpha|=1}} \left(\frac{2\pi}{(a_\alpha+2)n}\right)^{17n^4} \right\},$$

for all $n \leq N$ for some given N.

Proof. The constants C and $\mathrm{M}(f)$ are as before in previous results. In this bound we use tighter explicit constants for bounding the totient function and divisors function again computable by using Lemma 6.85 and Lemma 6.86. We now focus on bounding terms of the form $\Phi_n(\alpha)$ where $|\alpha| = 1$. We have

$$|\Phi_n(\alpha)| = \prod_{d|n} |\alpha^d - 1|^{\mu(n/d)}.$$

For $\mu(n/d) = 1$ we may use our estimate from Lemma 6.95 directly. For $\mu(n/d) = -1$ we have $|\alpha^d - 1|^{-1} \geq 1/2$, whereas for $n > 4$ we have $2\pi/(a+2)n < 1/2$, hence we may use the same lower bound estimate in the case $\mu(n/d) = -1$. This gives

$$|\Phi_n(\alpha)| = \prod_{d|n} |\alpha^d - 1|^{\mu(n/d)} \geq \prod_{d|n} \left(\frac{2\pi}{(a_\alpha+2)d}\right) \geq \prod_{d|n} \left(\frac{2\pi}{(a_\alpha+2)d}\right)$$
$$= \left(\frac{2\pi}{(a_\alpha+2)d}\right)^{\mathrm{d}(n)} \geq \left(\frac{2\pi}{(a_\alpha+2)d}\right)^{17n^4}.$$

The bound now immediately follows. □

We now apply this bound to the case $f_{3,7}(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1$.

Corollary 6.97. *For $150,000 \leq n \leq 10^{76}$ each a_n has at least one primitive prime factor.*

Proof. We apply the bound from Lemma 6.96 to show that $|a_n| > n^6$ within this range of n. □

Combining Corollary 6.97 and Proposition 6.93 we have that a_n has a primitive prime divisor for all $n \geq 150,000$. The number 150,000 is small enough that we may now complete our investigation by computing a_n for $1 \leq n < 150,000$ and determining which a_n have primitive prime divisors. This gives the following result.

Proposition 6.98. *For* $f_{3,7}(x) = x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1$ *each* a_n *has a primitive prime divisor for*

$$n \notin \{1, 2, 3, 4, 5, 6, 7, 10, 11, 16, 17, 18, 24, 27, 36, 38, 56, 60, 78\}.$$

Hence we may state our result as it relates to regular maps.

Corollary 6.99. *For all* $m \geq 7$ *and*

$$m \notin \{7, 10, 11, 16, 17, 18, 24, 27, 36, 38, 56, 60, 78\}$$

there exists a $(3, 7, m)$*-regular map with automorphism group a fractional linear group.*

Applying the same logic to all cases of $k, l \leq 10$ we find the following exceptional cases in which (k, l, m)-regular maps do not exist in fractional linear groups.

k	l	Exceptions
3	7	1, 2, 3, 4, 5, 6, 7, 10, 11, 16, 17, 18, 24, 27, 36, 38, 56, 60, 78
3	8	1, 2, 3, 4, 5, 6, 9, 12, 14, 24, 30, 60
3	9	1, 2, 3, 4, 5, 6, 8, 11, 12, 14, 28, 30, 36
3	10	1, 2, 3, 4, 5, 6, 7, 10, 18, 24, 30
4	5	1, 2, 3, 4, 5, 7, 10, 18, 24, 30
4	6	1, 2, 3, 4, 6, 12
4	7	1, 2, 3, 4, 5, 7, 18
4	8	1, 2, 3, 4, 8, 10
4	9	1, 2, 3, 4, 9
4	10	1, 2, 3, 4, 5, 8, 20, 30
5	5	1, 2, 3, 4, 6, 7, 8, 15
5	6	1, 2, 3, 5, 8, 10, 20, 30
5	7	1, 2, 3, 4, 5, 8
5	8	1, 2, 3, 5, 6, 7, 12, 20
5	9	1, 2, 3, 42
5	10	1, 2, 3, 4, 6, 10
6	6	1, 2, 3, 4
6	7	1, 2, 3
6	8	1, 2, 3, 5, 8, 12
6	9	1, 2, 3, 18
6	10	1, 2, 3, 5
7	7	1, 2, 3, 4, 8
7	8	1, 2, 5, 7
7	9	1, 2, 12
7	10	1, 2, 3
8	8	1, 2, 4, 6
8	9	1, 2, 3
8	10	1, 2, 4
9	9	1, 2, 4, 12
9	10	1, 2, 12
10	10	1, 2, 3, 5

In addition to our ability to, for a fixed pair $(k, l) \in \mathbb{N}^2$, calculate explicitly the set of all m such that no (k, l, m)-regular map exists in fractional linear groups, we are also able to calculate explicit examples of (k, l, m)-maps where they do exist in fractional linear groups. To do this, we first calculate $N(k, l, m)$; then, for each prime $p \mid N(k, l, m)$, we calculate all solutions to $\omega_k + \omega_l + \omega_m + 2 = 0$ in finite fields of characteristic p; then finally we may use our values for ω_k, ω_l and ω_m in our explicit forms of the generator matrices X, Y and Z to give explicit descriptions of our groups. We now give some example maps.

Let $F = \mathrm{GF}(7^2)$, and $\alpha \in F$ be a root of $x^2 + 6x + 3$. Define $X, Y, Z \in \mathrm{SL}(2, 7^2)$ by

$$X = \begin{pmatrix} 0 & 6\alpha + 4 \\ 6\alpha + 4 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 4\alpha + 5 & \alpha + 3 \\ 6\alpha + 4 & 3\alpha + 2 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 0 & 5\alpha + 1 \\ 3\alpha + 2 & 0 \end{pmatrix}.$$

Then the group $G = \langle \bar{X}, \bar{Y}, \bar{Z} \rangle \leq \mathrm{PSL}(2, 7^2)$ is the automorphism group of a $(3, 7, 8)$-regular map. In particular we have $\mathrm{ord}(\bar{X}\bar{Y}) = 7$, $\mathrm{ord}(\bar{Y}\bar{Z}) = 3$ and $\mathrm{ord}(\bar{Z}\bar{X}\bar{Y}) = 8$.

Let $F = \mathrm{GF}(5^2)$, and $\alpha \in F$ be a root of $x^2 + 4x + 2$. Define $X, Y, Z \in \mathrm{SL}(2, 5^2)$ by

$$X = \begin{pmatrix} 0 & 3\alpha + 1 \\ 4\alpha + 3 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}.$$

Then the group $G = \langle \bar{X}, \bar{Y}, \bar{Z} \rangle \leq \mathrm{PSL}(2, 5^2)$ is the automorphism group of a $(4, 5, 6)$-regular map. In particular we have $\mathrm{ord}(\bar{X}\bar{Y}) = 5$, $\mathrm{ord}(\bar{Y}\bar{Z}) = 4$ and $\mathrm{ord}(\bar{Z}\bar{X}\bar{Y}) = 6$.

Let $F = GF(7^2)$ and $\alpha \in F$ be a root of $x^2 + 6x + 3$. Define $X, Y, Z \in \mathrm{SL}(2, 7^2)$ by

$$X = \begin{pmatrix} 6\alpha + 4 & 0 \\ 5\alpha + 1 & \alpha + 3 \end{pmatrix}, \quad Y = \begin{pmatrix} 6\alpha + 4 & \alpha + 3 \\ 0 & \alpha + 3 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 6\alpha + 4 & 0 \\ 0 & \alpha + 3 \end{pmatrix}.$$

The the group $G = \langle \bar{X}, \bar{Y}, \bar{Z} \rangle \leq \mathrm{PSL}(2, 7^2)$ is the automorphism group of a $(7, 7, 6)$-regular map. In particular we have $\mathrm{ord}(\bar{X}\bar{Y}) = 7$, $\mathrm{ord}(\bar{Y}\bar{Z}) = 7$ and $\mathrm{ord}(\bar{Z}\bar{X}\bar{Y}) = 6$.

6.6 Prime Cases

Finally we conclude our discussion of (k, l, m)-regular maps in fractional linear groups by considering the case in which each of k, l and m is a prime number. In this case we are able to say a little more than previously regarding the conditions for the existence of a (k, l, m)-regular map in fractional linear groups.

Throughout this section we shall consider (p, q, r)-regular maps where we assume $p \neq q$ and that p, q is a hyperbolic pair. First we require the following lemma. In the following we use the notation $\Gamma(L/K)$ to denote the Galois group of the field L over the field K.

Lemma 6.100. $[\mathbb{Q}(\omega_p + \omega_q) : \mathbb{Q}] = (p - 1)(q - 1)/4$.

Proof. In the case where $p = 3$ we have $\omega_p = 1$ and the result is trivial. Hence we assume that $p, q > 3$. To show the result we shall use the following facts

i) if $L : K$ is a normal extension of K, and M is an intermediate field $K \subseteq M \subseteq L$, then $[L : M] = |\Gamma(L/M)|$;

ii) the field extension $\mathbb{Q}(\xi_{pq}) : \mathbb{Q}$ is a normal extension and $[\mathbb{Q}(\xi_{pq}) : \mathbb{Q}] = (p-1)(q-1)$;

iii) $\mathbb{Q}(\xi_p) \cap \mathbb{Q}(\xi_q) = \mathbb{Q}$.

Our strategy is to calculate $[\mathbb{Q}(\xi_{pq} : \mathbb{Q}(\omega_p + \omega_q)]$ by explicitly calculating $G = \Gamma(\mathbb{Q}(\xi_{pq})/\,\mathbb{Q}(\omega_p + \omega_q))$. We know that each automorphism $\phi \in H = \Gamma(\mathbb{Q}(\xi_{pq})/\,\mathbb{Q})$ is uniquely defined by some n coprime to pq and the fact for any pq^{th} root of unity ξ we have $\phi(\xi) = \xi^n$. From the Galois correspondence we know that $G \subseteq H$. If $\phi \in G$, then we must have $\phi(\omega_p + \omega_q) = \omega_p + \omega_q$, as G fixes $\mathbb{Q}(\omega_p + \omega_q)$, and further we know that if $\phi \in H$ and $\phi(\omega_p + \omega_q) = \omega_p + \omega_q$ then ϕ fixes $\mathbb{Q}(\omega_p + \omega_q)$. Therefore, $G = \{\phi \in H | \phi(\omega_p + \omega_q) = \omega_p + \omega_q\}$. We now find all such ϕ. Suppose $\phi \in H$ and $\phi(\omega_p + \omega_q) = \omega_p + \omega_q$. We may choose ξ_{pq} such that $\omega_p = \xi_{pq}^q + \xi_{pq}^{-q}$ and $\omega_q = \xi_{pq}^p + \xi_{pq}^{-p}$. Let n be the unique number $1 \leq n < pq$ such that $(n, pq) = 1$ and $\phi(\xi_{pq}) = \xi_{pq}^n$. This gives us

$$\begin{aligned}\xi_{pq}^q + \xi_{pq}^{-q} + \xi_{pq}^p + \xi_{pq}^{-p} = \omega_p + \omega_q = \phi(\omega_p + \omega_q) &= \phi(\xi_{pq}^q) + \phi(\xi_{pq}^{-q}) + \phi(\xi_{pq}^p) + \phi(\xi_{pq}^{-p}) \\ &= \xi_{pq}^{nq} + \xi_{pq}^{-nq} + \xi_{pq}^{np} + \xi_{pq}^{-np}\end{aligned}$$

We may rearrange this equation to the following

$$\xi_p + \xi_p^{-1} + \xi_p^n + \xi_p^{-n} = \xi_q + \xi_q^{-1} + \xi_q^n + \xi_q^{-n},$$

where $\xi_p = \xi_{pq}^q$ and $\xi_q = \xi_{pq}^p$. As the left hand side is in $\mathbb{Q}(\xi_p)$ and the right hand side is in $\mathbb{Q}(\xi_q)$, we must have that both sides are in $\mathbb{Q}(\xi_p) \cap \mathbb{Q}(\xi_q) = \mathbb{Q}$. As one of $p, q > 5$, without loss of generality take $p > 5$. We know that the p^{th} roots of unity form a set of more than four algebraic numbers linearly independent over $\mathbb{Q}$ and so a sum of at most 4 distinct p^{th} roots of unity equal to a number in $\mathbb{Q}$ must be a trivial sum and equal to zero. This gives us

$$\xi_p + \xi_p^{-1} + \xi_p^n + \xi_p^{-n} = \xi_q + \xi_q^{-1} + \xi_q^n + \xi_q^{-n} = 0.$$

Hence we have

$$\xi_p + \xi_p^{-1} = \xi_p^n + \xi_p^{-n} \quad \text{and} \quad \xi_q + \xi_q^{-1} = \xi_q^n + \xi_q^{-n}.$$

From the left hand side we deduce that $n \equiv \pm 1 \pmod{p}$, and from the right hand side we deduce $n \equiv \pm 1 \pmod{q}$. It is now trivial to show that this gives us exactly four distinct automorphisms. Therefore, $|G| = 4$, and hence we have

$$(p-1)(q-1) = [\mathbb{Q}(\xi_{pq}) : \mathbb{Q}] = [\mathbb{Q}(\xi_{pq}) : \mathbb{Q}(\omega_p + \omega_q)][\mathbb{Q}(\omega_p + \omega_q) : \mathbb{Q}] = 4[\mathbb{Q}(\omega_p + \omega_q) : \mathbb{Q}],$$

and so $[\mathbb{Q}(\omega_p + \omega_q) : \mathbb{Q}] = (p-1)(q-1)/4$. □

This allows us to give the following important corollary.

Corollary 6.101. *The polynomial $f_{p,q}(x)$ is irreducible.*

Proof. Let α be a root of a factor $x^2 + (\omega_p + \omega_q + 2)x + 1$ of $f_{p,q}(x)$ for $\omega_p + \omega_q < 0$. We consider $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. First, we have that $\deg(f_{p,q}(x)) = (p-1)(q-1)/2$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = (p-1)(q-1)/2$ if, and only if, $f_{p,q}(x)$ is irreducible. We have that $\alpha + \alpha^{-1} = -(\omega_p + \omega_q + 2)$, hence $\mathbb{Q}(\omega_p + \omega_q) \subseteq \mathbb{Q}(\alpha)$. Further, as we chose $\omega_p + \omega_q < 0$, we must have $\alpha \in \mathbb{C} \setminus \mathbb{R}$, so $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\omega_p + \omega_q)$. Hence, as $g(x) = x^2 + (\omega_p + \omega_q + 2)x + 1 \in \mathbb{Q}(\omega_p + \omega_q)[x]$ we have that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\omega_p + \omega_q)] = 2$, and so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\omega_p + \omega_q)][\mathbb{Q}(\omega_p + \omega_q) : \mathbb{Q}] = (p-1)(q-1)/2,$$

showing that $f_{p,q}(x)$ is irreducible. □

This gives us the further important corollary.

Corollary 6.102. *No cyclotomic polynomial $\Phi_n(x)$ satisfies $\Phi_n(x) \mid f_{p,q}(x)$.*

Proof. We know from Corollary 6.101 that $f_{p,q}(x)$ is irreducible, and from Lemma 6.58 that $f_{p,q}(x)$ has at least one irreducible factor $g(x)$ such that $Phi_n(x) \nmid g(x)$ and $x \nmid g(x)$. Hence $f_{p,q}(x)$ satisfies $\Phi_n(x) \nmid f_{p,q}(x)$ for any n. □

We now give our condition for the existence of a (p, q, r)-regular map in fractional linear groups.

Proposition 6.103. *There is a (p, q, r)-regular map in fractional linear groups if, and only if,*

$$a_r = \prod_{\alpha \in \rho(f_{p,q})} \Phi_r(\alpha) \neq 1.$$

Proof. We first show that $a_r \geq 0$. To show this, we show that $a_m > 0$ in the series corresponding to the polynomial $f_{k,l}(x)$ for arbitrary k and l.

$$a_m = \prod_{\alpha \in \rho(f_{k,l})} \Phi_m(\alpha) = (-1)^{\deg(\Phi_m)\deg(f_{k,l})} \prod_{\xi_m \in \rho(\Phi_m)} f_{k,l}(\xi_m)$$

$$
\begin{aligned}
&= \prod_{\xi_m \in \rho(\Phi_m)} \left(\prod_{\substack{\omega_k \in \rho(\Psi_k) \\ \omega_l \in \rho(\Psi_l)}} (\xi_m^2 + (\omega_k + \omega_l + 2)\xi_m + 1) \right) \\
&= \prod_{\xi_m + \xi_m^{-1} \in \rho(\Psi_m)} \Big(\prod (\xi_m^2 + (\omega_k + \omega_l + 2)\xi_m + 1)(\xi_m^{-2} + (\omega_k + \omega_l + 2)\xi_m^{-1} + 1) \Big) \\
&= \prod \Big(\prod \xi_m (\xi_m + (\omega_k + \omega_l + 2) + \xi_m^{-1}) \xi_m^{-1} (\xi_m^{-1} + (\omega_k + \omega_l + 2) + \xi_m) \Big) \\
&= \prod_{\substack{\omega_k \in \rho(\Phi_k) \\ \omega_l \in \rho(\Phi_l) \\ \omega_m \in \rho(\Phi_m)}} (\omega_k + \omega_l + \omega_m + 2)^2 = N(k,l,m)^2.
\end{aligned}
$$

We have $\deg(f_{k,l}(x)) = 2\deg(\Psi_k)\deg(\Psi_l)$ and is even, giving us $a_m \geq 0$.

Returning to the case $k = p$, $l = q$ and $m = r$ where p, q and r are primes with $p \neq q$ and p, q is a hyperbolic pair. We have that $a_r = 0$ if, and only if, $\Phi_r(x)$ and $f_{p,q}(x)$ share a common root. From Corollary 6.102 we have that there is no $\Phi_n(x)$ such that $\Phi_n(x) \mid f_{p,q}(x)$, so $f_{p,q}(x)$ and $\Phi_r(x)$ share no common root and we have $a_r \neq 0$. Hence we have $a_r \geq 1$. Now suppose $\pi \mid a_r$. From Proposition 6.11 we see that for each $n \in \{p, q, r\}$ we have either $\pi \nmid n$ or $\pi = n$, and further as $p \neq q$ we do not have $(p, q, r) = (\pi, \pi, \pi)$. Therefore, if there is some prime π such that $\pi \mid a_r$ then there exists a (p, q, r)-regular map. □

This proposition gives our most promising avenue for investigation to provide a proof on existence of finite (k, l, m)-regular maps for all triples (k, l, m) apart from some small exceptions. If one can show that for all but a few exceptions we have $a_r \neq 0$, then (p, q, r)-regular maps will be useful to build maps for arbitrary (k, l, m). Further, through searching all triples (p, q, r) with $p \neq q$ and $p, q, r \leq 50$ the only exceptions for which (p, q, r)-regular maps do not exist are the following

$$(3,7,7), (3,7,11), (3,7,17), (3,11,13), (3,11,23), (5,5,7).$$

Hence it may be possible to show directly that $a_r \neq 1$ for all $p, q > 5$.

Chapter 7

Regular Maps with Trinity Symmetry

7.1 Introduction

In this chapter we shall consider the question of for which $n \in \mathbb{N}$ there exist (n, n, n)-regular maps which are both self dual and self Petrie dual. Prior to our work, the problem had already been settled for even n by Archdeacon, Conder and Širáň in [1]. For odd n, the problem was settled by Širáň, Jeans, Erskine, Hriňáková and the author in [28, 22]. In [22] Erskine, Hriňáková and Jeans establish sufficient conditions for the existence of an (n, n, n)-regular map in fractional linear groups. The condition they provide is that if there is some finite field K of characteristic p and some element $\omega = \xi + \xi^{-1}$ for $\xi \in K$ where ξ has multiplicative order $2n$, and we have $3\omega^2 = 4$, then there is an (n, n, n)-regular map which is both self dual and self Petrie dual. Using this condition, in [28] the question of whether there exist self dual and self Petrie dual (n, n, n)-regular maps is resolved by showing that there exist solutions to $3\omega^2 = 4$ for each prime $n > 3$. Once this is shown, another argument is used to show that if a self dual, self Petrie dual (n, n, n)-regular map exists then for any $k \in \mathbb{N}$ a self dual, self Petrie dual (kn, kn, kn)-regular map exists, thus resolving the question.

We now address this question using the methods of the previous chapter to show that there exist self dual, self Petrie dual (n, n, n)-regular maps for all but finitely many values n which we shall explicitly calculate.

7.2 Application of Earlier Results

We first begin with a small lemma.

Lemma 7.1. *There is some $\xi \in K$ of order $2n$ such that $3\omega^2 = 4$ if, and only if, there is a root of order n to the polynomial $f(x) = 3x^2 + 2x + 3$ in K.*

Proof. We have

$$3\omega^2 = 4 \quad \Leftrightarrow \quad 3\xi^2 + 6 + 3\xi^{-2} = 4 \quad \Leftrightarrow \quad 3\xi^4 + 2\xi^2 + 3 = 0.$$

Letting $\zeta = \xi^2$ we have that ζ has multiplicative order n and $0 = 3\zeta^2 + 2\zeta + 3 = f(\zeta)$.

Conversely, suppose that ζ is a root of $f(x)$ of order n. There are two numbers ξ such that $\xi^2 = \zeta$, at least one of which is order $2n$, hence let ξ satisfy $\xi^2 = \zeta$ and $\mathrm{ord}(\xi) = 2n$. We easily see that $3\omega^2 = 4$ in K. □

Hence, from now on we consider the polynomial $f(x) = 3x^2 + 2x + 3$ and the question of finding roots of $f(x)$ of particular multiplicative order. Let α and β be the roots of $f(x)$. As before, we define sequences $\langle A_n \rangle$ and $\langle a_n \rangle$. However, as $f(x)$ is not monic we must make an adjustment from our previous definition.

$$A_n = 3^n(\alpha^n - 1)(\beta^n - 1) \quad \text{and} \quad a_n = 3^{\varphi(n)}\Phi_n(\alpha)\Phi_n(\beta).$$

We have the following properties of the sequences $\langle A_n \rangle$ and $\langle a_n \rangle$.

Lemma 7.2. *The sequences $\langle A_n \rangle$ and $\langle a_n \rangle$ satisfy the following properties.*

i) $A_n, a_n \in \mathbb{Z}$ *for all* $n \geq 0$*;*

ii) $A_n = \prod_{d|n} a_d$*;*

iii) there is a root of order n in a finite field of characteristic p if, and only if, $p \nmid n$ and $p \mid a_n$;

iv) if $p \mid a_{pn}$ then $p \mid a_n$;

v) for each p there exists either one or two numbers k such that $p \mid a_n$ implies $n = kp^r$ for some $r \geq 0$;

vi) $A_0 = 0$, $A_1 = 8$, $A_2 = 32$ *and* $A_{n+3} = A_{n+2} - 3A_{n+1} + 27A_n$.

Proof. The proofs of these points follows Lemma 6.35. We explicitly prove point (vi) as follows. We have $A_n = 3^n(\alpha^n - 1)(\beta^n - 1) = 2 \times 3^n - (3\alpha)^n - (3\beta)^n$, hence letting $g(x) = (x-3)(x-3\alpha)(x-3\beta) = x^3 - x^2 + 3x - 27$ we have $g(3) = g(3\alpha) = g(3\beta) = 0$ and hence $C\gamma^{n+3} = C\gamma^{n+2} - 3C\gamma^{n+1} + 27C\gamma$ for each $\gamma \in \{3, 3\alpha, 3\beta\}$. Hence we have

$$\begin{aligned}
&A_{n+2} - 3A_{n+1} + 27A_n \\
=&(2 \times 3^{n+2} - (3\alpha)^{n+2} - (3\beta)^{n+2}) - 3(2 \times 3^{n+1} - (3\alpha)^{n+1} - (3\beta)^{n+1}) \\
&\quad + 27(2 \times 3^n - (3\alpha)^n - (3\beta)^n) \\
=&2 \times 3^n(3^2 - 3 \times 3 + 27) - (3\alpha)^n((3\alpha)^2 - 3(3\alpha) + 27) \\
&\quad - (3\beta)^n((3\beta)^2 - 3(3\beta) + 27) \\
=&2 \times 3^{n+3} - (3\alpha)^{n+3} - (3\beta)^{n+3} = A_{n+3}.
\end{aligned}$$

We get $A_0 = 0$, $A_1 = 8$ and $A_2 = 32$ by simple calculation. □

As before, we shall call a prime p such that $p \nmid n$ and $p \mid a_n$ a *primitive prime divisor* of a_n. Again, we aim to give an upper bound on a_n with no primitive prime divisors. We start with the following lemma.

Lemma 7.3. *For any prime $p \notin \{2, 3\}$ if $p \mid n$ then $p^3 \nmid a_n$.*

Proof. The proof of Proposition 6.72 may be applied for all primes p such that both $p \nmid \Delta_f = -32$, the discriminant of $f(x)$, and the lead coefficient of $f(x)$ is non-zero in $\mathbb{Z}/p\mathbb{Z}$. Hence we may apply Proposition 6.72 for all $p \notin \{2, 3\}$. □

We now settle the cases of $p \in \{2, 3\}$.

Lemma 7.4. *For all n we have $3 \nmid a_n$.*

Proof. From Lemma 7.2 we have that $A_n \pmod 3$ is given by

$$A_0 \equiv 0, \quad A_1 \equiv 2, \quad A_2 \equiv 2, \quad \text{and} \quad A_{n+3} \equiv A_{n+2} \pmod 3.$$

Hence we have $A_n \equiv 2 \pmod 3$ for all $n \geq 1$. Hence from the formula $A_n = \prod_{d|n} a_d$ we may deduce that $a_1 \equiv 2 \pmod 3$ and $a_n \equiv 1 \pmod 3$ for all $n \geq 2$. Hence we have $3 \nmid a_n$ for all $n \geq 1$. □

Lemma 7.5. *If $2 \mid n$ then $2^3 \nmid a_n$.*

Proof. First, we note from Lemma 7.2 that $2 \mid a_n$ and $2 \nmid n$ if, and only if, $f(x)$ has a root of order n in a finite field of characteristic 2. In GF(2) we have $f(x) = (x+1)^2$, hence we have $2 \mid a_n$ and $2 \nmid n$ implies $n = 1$. Combining this with the fact $2 \mid a_{2n}$ implies $2 \mid a_n$ we have $2 \mid a_n$ implies $n = 2^k$ for some $k \geq 0$. Further, we have

$$A_n = 3^n(\alpha^n - 1)(\beta^n - 1) = 2 \times 3^n - (3\alpha)^n - (3\beta)^n,$$

and hence

$$\begin{aligned} A_{2n} &= 3^{2n}(\alpha^{2n} - 1)(\beta^{2n} - 1) = 3^n(\alpha^n - 1)(\beta^n - 1)3^n(\alpha^n + 1)(\beta^n + 1) \\ &= A_n(2 \times 3^n + (3\alpha)^n + (3\beta)^n) = A_n(4 \times 3^n - A_n). \end{aligned}$$

Hence, as $A_1 = 8 = 2^3$, we may use induction to show that $2^{3+2k} \mid\mid A_{2^k}$ for $k \geq 0$, and hence we have $2^3 \mid\mid a_1$ and $2^2 \mid\mid a_{2^k}$ for $k \geq 1$. As $2 \nmid a_n$ for any $n \neq 2^k$ the result immediately follows. □

We now combine these lemmas to give our bound on $|a_n|$ when a_n has no primitive prime divisors.

Corollary 7.6. *If a_n has no primitive prime divisors then $|a_n| \leq \mathrm{rad}(n)^2$.*

Proof. Immediate from combining Lemma 7.3, Lemma 7.4 and Lemma 7.5. □

This completes our upper bound on $|a_n|$ when a_n has no primitive prime divisors. We now aim to create a lower bound on $|a_n|$.

Lemma 7.7. *We have the following inequality for $|a_n|$*

$$\begin{aligned}|a_n| &> 3^{\varphi(n)} \exp(-2\,\mathrm{d}(n)(A(7.5+\log n)^2+\log 2)) \\ &> 3^{\sqrt{n/2}} \exp(-8n^{1/3}(402000(7.5+\log n)^2+\log 2)).\end{aligned}$$

Proof. We have $a_n = 3^{\varphi(n)}\Phi_n(\alpha)\Phi_n(\beta)$, hence we use Lemma 6.80 to find a bound for $|\Phi_n(\alpha)|$, noting that $|\Phi_n(\beta)| = |\Phi_n(\alpha)|$ as α and β are complex conjugates. We calculate the constant A as follows. In Theorem 6.78 we take

i) $\alpha_1 = \alpha$, $\alpha_2 = 1$;

ii) $D = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$;

iii) $\log \alpha_1 = \log \alpha = 1.910\ldots i$, $\log \alpha_2 = \log 1 = 2\pi i$;

iv) $f = 2e$.

This gives $\mathrm{h}(\alpha_1) = \log 3/2$, and hence $a_1 = f|\log \alpha|/2 > \max(1, \mathrm{h}(\alpha) + 2)$, and $a_2 = f\pi > \max(1, \mathrm{h}(1))$. This gives us

$$A = 270D^4 a_1 a_2 = 270 \times 2^4 \times 4e^2 \times \pi < 402,000.$$

□

Proposition 7.8. *For all $n \geq 10^{67}$ there is at least one primitive prime divisor of a_n.*

Proof. We may use the bound of Lemma 7.7 to show that for all $n \geq 10^{67}$ we have $|a_n| > n^2 \geq \mathrm{rad}(n)^2$, and hence by Corollary 7.6 we see that a_n must have at least one primitive prime divisor. □

We now use the method of continued fractions to improve this bound.

Proposition 7.9. *For all* $16,767 \leq n \leq 10^{67}$ *there exists at least one primitive prime divisor of* a_n*.*

Proof. Taking a continued fraction expansion of α we find that in this range of n the following inequality applies

$$|a_n| \geq 3^{(1/5)n^{49/50}} \left(\frac{2\pi}{1220n}\right)^{17n^{1/4}}.$$

Using this inequality we may show $|a_n| > n^2$ within this range, from which we get the result. □

Finally, we may explicitly compute a_n for all $1 \leq n \leq 16,767$ in order to determine all n for which a_n has at least one primitive prime divisor.

Proposition 7.10. *For all* $n \notin \{2, 3, 4, 10\}$ *there is at least one primitive prime divisor of* a_n*.*

Proof. This is the combination of Proposition 7.8, Proposition 7.9 and a computer search. □

This now allows us to state our result regarding regular maps.

Proposition 7.11. *For all* $n \notin \{1, 2, 3, 4, 10\}$ *there exists an* (n, n, n)*-regular map which is both self dual and self Petrie dual whose automorphism group is a fractional linear group.*

We now give some examples of generators of automorphism groups of regular maps with trinity symmetry.

Let $X, Y, Z \in \mathrm{SL}(2, 11)$ be given by

$$X = \begin{pmatrix} 4 & 7 \\ 7 & 7 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 10 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 0 & 4 \\ 8 & 0 \end{pmatrix}.$$

The group $G = \langle \bar{X}, \bar{Y}, \bar{Z} \rangle \leq \mathrm{PSL}(2, 11)$ is the automorphism group of a $(5, 5, 5)$-regular map with trinity symmetry.

Let $F = \mathrm{GF}(5^2)$ and let $\alpha \in F$ be a root of $x^2 + 4x + 2$. Define X, Y and Z by

$$X = \begin{pmatrix} 4\alpha + 3 & \alpha + 1 \\ 2\alpha + 1 & \alpha + 2 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 3\alpha \\ \alpha + 4 & 0 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 0 & 3\alpha + 1 \\ 4\alpha + 3 & 0 \end{pmatrix}.$$

The group $\langle \bar{X}, \bar{Y}, \bar{Z} \rangle \leq \mathrm{PSL}(2, 5^2)$ is the automorphism group of a $(6, 6, 6)$-regular map with trinity symmetry.

Let $F = \mathrm{GF}(13^2)$ and let $\alpha \in F$ be a root of $x^2 + 12x + 2$. Define X, Y and Z by

$$X = \begin{pmatrix} 2\alpha + 12 & 10\alpha + 3 \\ \alpha & 11\alpha + 1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 6\alpha + 5 \\ 11\alpha + 8 & 0 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 0 & 6 \\ 2 & 0 \end{pmatrix}.$$

The group $\langle \bar{X}, \bar{Y}, \bar{Z} \rangle \leq \mathrm{PSL}(2, 13^2)$ is the automorphism group of a $(7, 7, 7)$-regular map with trinity symmetry.

Chapter 8

Conclusion

We now provide a brief summary of the work undertaken in this PhD.

Our work with Moore graphs and mixed Moore graphs both provided an alternate derivation of the Hoffman-Singleton graph and showed a fundamental similarity between the problem of determining Moore graphs of diameter 2 and mixed Moore graphs of diameter 2 and directed out degree 1. In this area, the important outstanding problems are the question of the existence of a $(57, 2)$-Moore graph and a $(21, 1, 2)$-mixed Moore graph. The problem of the potential existence of a $(57, 2)$-Moore graph is amongst the most famous open problems in algebraic graph theory, and therefore any results which may shed light on this problem are of great interest. The most powerful results concerning a potential $(57, 2)$-Moore graph currently known are that such a graph cannot be vertex transitive, proved by Higman in unpublished lectures, and that if such a graph exists its automorphism group must have at most 375 automorphisms, Mačaj and Širáň [41]. The most natural extension of our results which we have not explored is to attempt to modify the proofs of these facts to the case of a $(21, 1, 2)$-mixed Moore graph. In these case neither of the corresponding results is currently known. Further, as all known Moore and mixed Moore graphs are vertex transitive, one could attempt to prove that a $(21, 1, 2)$-mixed Moore graph would necessarily be vertex transitive. Hypothetically, if such a method of proof could be achieved for non-existence of a mixed Moore graph that would form an important contribution to the research into the degree diameter problem.

In our work on Gómez graphs we showed that the Gómez graphs are the extremal graphs for given degree and diameter for our definition of shift restricted word graphs. We also showed that the extremal Gómez graphs are not Cayley graphs. Unfortunately, however, our method of proof is difficult to apply in general, and indeed leaves the question of whether the non-extremal Gómez graphs are Cayley open. A natural question to pursue following our results is whether a simpler condition may be placed on the defining set of permutations for a word graph to determine whether it is Cayley. This would be of great help in eliminating the possibility of word graphs playing a role in forming the largest known Cayley graphs for given degree and diameter. Further, one could hope to show that no Gómez graphs are Cayley (beyond the exceptional cases already alluded to). Further to this, the

author is not aware of any research into non-shift restricted word graphs to see if they form an interesting category of graphs in relation to the degree diameter problem.

Our work into regular maps of given face, vertex and Petrie dual orders provides us a method to construct maps of given face, vertex and Petrie dual orders provided they exist in fractional linear groups, and allows us to determine exactly when such regular maps exist provided two of the parameters are fixed. However, the question of determining precisely when finite regular maps exist for given triples of face, vertex and Petrie dual orders remains open. We have provided a condition which, if true, will show there exist regular maps of arbitrary face, vertex and Petrie dual orders where each parameter is a prime greater than five and not all parameters are the same. If this condition can be shown to be true then our work may provide a valuable first step in resolving the problem. However, if a proof of this condition remains elusive then our work may indicate another approach is required to address this problem. With regards to investigating other approaches, the fact the method we provided may be altered to be constructive will allow the construction of example regular maps for given parameters, which may prove useful in further research into the question.

The related work undertaken regarding demonstrating when regular maps exhibiting trinity symmetry exist in fractional linear groups fully addresses the given problem. Further work in this area may include considering further symmetries that a regular map may exhibit and providing similar constructions in fractional linear groups. However, on this note it has been shown recently that there do not exist kaleidoscopic regular maps in fractional linear groups, and hence this approach will not always be applicable.

Bibliography

[1] Dan Archdeacon, Marston Conder, and Jozef Širáň, *Trinity symmetry and kaleidoscopic regular maps*, Transactions of the American Mathematical Society **366** (2014), 4491–4512.

[2] Jernej Azarija and Sandi Klavžar, *Moore graphs and cycles are extremal graphs for convex cycles*, Journal of Graph Theory **80** (2014), 34–42.

[3] Alan Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204–216.

[4] ———, *Linear forms in the logarithms of algebraic numbers (ii)*, Mathematika **14** (1967), 102–107.

[5] ———, *Linear forms in the logarithms of algebraic numbers (iii)*, Mathematika **14** (1967), 220–228.

[6] E. Bannai and T. Ito, *On finite Moore graphs*, Journal of the Faculty of Science of the University of Tokyo (1973), 191,208.

[7] Juraj Bosák, *Partially directed Moore graphs*, Mathematica Slovaca **29** (1979), 181–196.

[8] W. G. Bridges and S. Toueg, *On the impossibility of directed Moore graphs*, Journal of Combinatorial Theory (1980), 339–341.

[9] R. P. Bryant and D. Singerman, *Foundations of the theory of maps on surfaces with boundary*, Quart. J. Math. Oxford Ser. **36** (1985), 17–41.

[10] Peter J. Cameron, *Permutation groups*, Cambridge University Press, 1999.

[11] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Annals of Mathematics (1913), 30–48.

[12] F. Comellas and M. A. Fiol, *Vertex symmetric digraphs with small diameter*, Discrete Applied Mathematics **58** (1995), 1–12.

[13] Marston Conder, *Non-orientable regular maps of genus 2 to 202*, 2006.

[14] ———, *Orientable regular maps of genus 2 to 101*, 2006.

[15] Marston Conder, Nigel Boston, Gabino González-Diez, Gareth Jones, and Thomas Tucker, *Symmetries of surfaces, maps and dessins*.

[16] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular hypermaps over projective linear groups*, Journal of the Australian Mathematical Society (2008), 155–175.

[17] H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups*, Springer, 1972.

[18] R. M. Damerell, *On Moore graphs*, Mathematical Proceedings of the Cambridge Philosophical Society (1973), 227,236.

[19] Antonio Breda D'Azevedo, Roman Nadela, and Jozef Širáň, *Classification of regular maps of negative prime euler characteristic*, Transactions of the American Mathematical Society (2004), 4175,4190.

[20] John D. Dixon and Brian Mortimer, *Permutation groups*, Springer, 1996.

[21] Arnaud Durand, *Topics in metric number theory*.

[22] Grahame Erskine, Katarína Hriňáková, and Olivia Jeans, *Self-dual, self-Petrie-dual and Möbius regular maps on linear fractional groups*.

[23] Jan-Hendrik Evertse, *Linear forms in logarithms*.

[24] V. Faber and J. W. Moore, *High-degree low-diameter interconnection networks with vertex symmetry: The directed case*, Techincal Report LA-UR-88-1051, Los Alamos National Laboratory (1988).

[25] V. Faber, J. W. Moore, and W. Y. C. Chen, *Cycle prefix digraphs for symmetric interconnection networks*, Networks 23 (1993), 641,649.

[26] Sergio Falcon and Ángel Plaza, *Fibonacci series modulo m*, The American Mathematical Monthly **67** (1960), 525–532.

[27] ———, *k-fibonacci sequences modulo m*, Chaos, Solitions and Fractals (2009).

[28] Jay Fraser, Olivia Jeans, and Jozef Širáň, *Regular self-dual and self-Petrie-dual maps of arbitrary valency*, Ars Mathematica Contemporanea **16** (2019), 403–410.

[29] J. Gómez, *Large vertex symmetric digraphs*, Networks **50** (2007), 241–250.

[30] Paul R. Hafner, *The hoffman-singleton graph and its automorphisms*, Journal of Algebraic Combinatorics (2002), 7–12.

[31] Alan J. Hoffman and Robert R. Singleton, *On Moore graphs with diameters 2 and 3*, IBM Journal of Research and Development (1960), 497,504.

[32] L. O. James, *A combinatorial proof that the Moore (7, 2) graph is unique*, Utilitas Mathematica, Vol. 5 (1974), 79,84.

[33] G. A. Jones and D. Singerman, *Theory of maps on orientable surfaces*, Proc. London Math. Soc. **37** (1978), 273–307.

[34] Gareth A. Jones, Martin Mačaj, and Jozef Širáň, *Nonorientable regular maps over linear fractional groups*, Ars Mathematica Contemporanea (2012), 25,35.

[35] Leif K. Jørgensen, *New mixed Moore graphs and directed strongly regular graphs*, Discrete Mathematics **338** (2015), 1011–1016.

[36] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Annals of Mathematics (1933), 461–479.

[37] ———, *A note on trigonometric algebraic numbers*, The American Mathematical Monthly (1933), 165–166.

[38] Nacho López, Josep M. Miret, and Cèsar Fernández, *Non existence of some mixed Moore graphs of diameter 2 using SAT*, Discrete Mathematics **339** (2016), 589–596.

[39] Nacho López and Jordi Pujolàs, *Properties of mixed Moore graphs of directed degree one*, Discrete Mathematics **338** (2015), 522–526.

[40] E. Loz, H. Pérez-Rosés, and G. Pineda-Villavicencio, *combinatoricswiki.org*.

[41] Martin Mačaj and Jozef Širáň, *Search for the properties of the missing Moore graph*, Linear Algebra and its Applications (2009), 2381,2398.

[42] Maurice Mignotte and Michel Waldschmidt, *Linear forms in two logarithms and schneider's method*, Annales de la Faculté des Sciences de Toulouse (1989), 43–75.

[43] Mirka Miller and Jozef Širáň, *Moore graphs and beyond: A survey of the degree/diameter problem*, The Electronic Journal of Combinatorics (2013).

[44] Minh Hoang Nguyen, Mirka Miller, and Joan Gimbert, *On mixed Moore graphs*, Discrete Mathematics **307** (2007), 964–970.

[45] Tracy A. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Annals of Mathematics (1916), 53–64.

[46] J. Plesník and Š. Znám, *Strongly geodetic directed graphs*, Acta FRN Univ. Comen.-Mathematica **29** (1974), 29–34.

[47] Will Sawin, Private Communication.

[48] ———, *The resultant of an arbitrary polynomial and a cyclotomic polynomial*, MathOverflow, URL:https://mathoverflow.net/q/98149 (version: 2017-04-13).

[49] Andrew Vince, *Regular combinatorial maps*, Journal of Combinatorial Theory **35** (1983), 256–277.

[50] Mária Ždímalová and Ľubica Staneková, *Which Faber-Moore-Chen digraphs are Cayley digraphs?*, Discrete Mathematics (2010), 2238–2240.

[51] Steve Wilson, *Applications and refinements of vince's construction*, Geometriae Dedicata (1993), 231–242.

[52] Minoru Yabuta, *A simple proof of carmichael's theorem on primitive divisors*, The Fibonacci Quarterly (2001), 439–443.

[53] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Hamburg **11** (1936).